**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K 9/00 — A1

(11) International Publication Number: **WO 00/31677**

(43) International Publication Date: 2 June 2000 (02.06.00)

(21) International Application Number: PCT/US99/13049

(22) International Filing Date: 9 June 1999 (09.06.99)

(30) Priority Data:
60/109,287 20 November 1998 (20.11.98) US
60/131,014 26 April 1999 (26.04.99) US

(71)(72) Applicant and Inventor: BEECHAM, James, E. [US/US]; 8820 Cortile Drive, Las Vegas, NV 89134 (US).

(74) Agent: PARSONS, Robert, A.; Suite 260, 340 East Palm Lane, Phoenix, AZ 85004 (US).

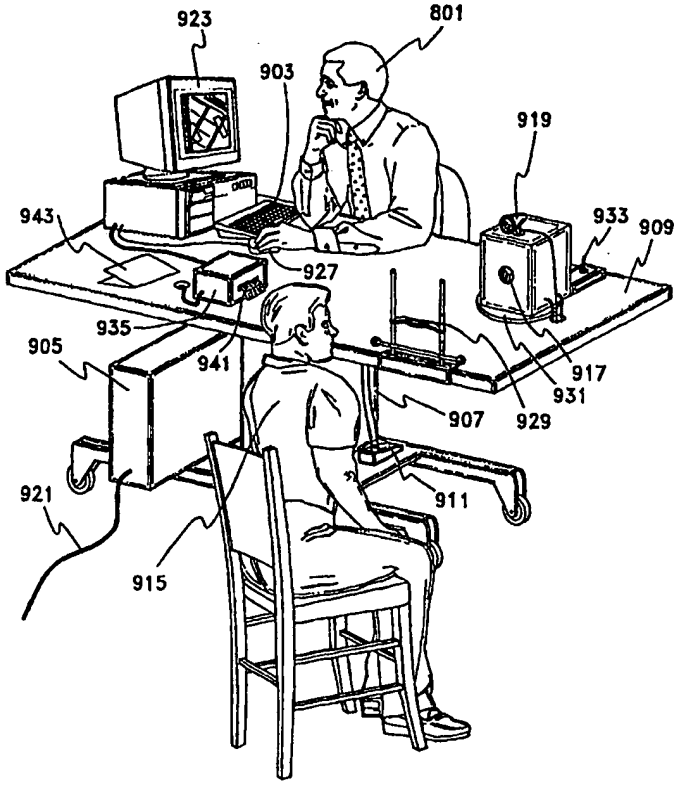
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published**
*With international search report.*

(54) Title: METHOD, SYSTEM AND APPARATUS FOR AUTHORIZATION AND VERIFICATION OF DOCUMENTS

(57) Abstract

A method for the authorization of documents is disclosed which includes preparing a record for future reference by authorized personnel including providing a sensitive document (943), collecting biometric data (917) from an individual (915) requesting authority to become an authorized person to access the document (943), forming a bar code (941) including the biometric data from the individual, attaching the bar code to the document (943), and storing the document and attached bar code. Access to the document is authorized by collecting current biometric data from a person requesting access, comparing the current biometric data to the bar code attached to the document, and confirming that the person requesting access and the authorized individual are identical. Included is a method in which portions of a digital photograph are linked to different biometric data and stored data is compared to current data with the linked portions being joined to make a composite photograph.



*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **AL** | Albania | **ES** | Spain | **LS** | Lesotho | **SI** | Slovenia |
| **AM** | Armenia | **FI** | Finland | **LT** | Lithuania | **SK** | Slovakia |
| **AT** | Austria | **FR** | France | **LU** | Luxembourg | **SN** | Senegal |
| **AU** | Australia | **GA** | Gabon | **LV** | Latvia | **SZ** | Swaziland |
| **AZ** | Azerbaijan | **GB** | United Kingdom | **MC** | Monaco | **TD** | Chad |
| **BA** | Bosnia and Herzegovina | **GE** | Georgia | **MD** | Republic of Moldova | **TG** | Togo |
| **BB** | Barbados | **GH** | Ghana | **MG** | Madagascar | **TJ** | Tajikistan |
| **BE** | Belgium | **GN** | Guinea | **MK** | The former Yugoslav Republic of Macedonia | **TM** | Turkmenistan |
| **BF** | Burkina Faso | **GR** | Greece | | | **TR** | Turkey |
| **BG** | Bulgaria | **HU** | Hungary | **ML** | Mali | **TT** | Trinidad and Tobago |
| **BJ** | Benin | **IE** | Ireland | **MN** | Mongolia | **UA** | Ukraine |
| **BR** | Brazil | **IL** | Israel | **MR** | Mauritania | **UG** | Uganda |
| **BY** | Belarus | **IS** | Iceland | **MW** | Malawi | **US** | United States of America |
| **CA** | Canada | **IT** | Italy | **MX** | Mexico | **UZ** | Uzbekistan |
| **CF** | Central African Republic | **JP** | Japan | **NE** | Niger | **VN** | Viet Nam |
| **CG** | Congo | **KE** | Kenya | **NL** | Netherlands | **YU** | Yugoslavia |
| **CH** | Switzerland | **KG** | Kyrgyzstan | **NO** | Norway | **ZW** | Zimbabwe |
| **CI** | Côte d'Ivoire | **KP** | Democratic People's Republic of Korea | **NZ** | New Zealand | | |
| **CM** | Cameroon | | | **PL** | Poland | | |
| **CN** | China | **KR** | Republic of Korea | **PT** | Portugal | | |
| **CU** | Cuba | **KZ** | Kazakstan | **RO** | Romania | | |
| **CZ** | Czech Republic | **LC** | Saint Lucia | **RU** | Russian Federation | | |
| **DE** | Germany | **LI** | Liechtenstein | **SD** | Sudan | | |
| **DK** | Denmark | **LK** | Sri Lanka | **SE** | Sweden | | |
| **EE** | Estonia | **LR** | Liberia | **SG** | Singapore | | |

# METHOD, SYSTEM AND APPARATUS FOR AUTHORIZATION AND VERIFICATION OF DOCUMENTS

## Field of the Invention

This invention relates to novel methods, systems and apparatus for preparing, linking, filing, accessing, sorting, retrieving, transmitting and auditing documents, including reports, collections of data, etc., and, more particularly, to systems, apparatus and methods for linking legal documents to the identity of the individuals who are authorized access to said documents and reports. The instant invention further includes a novel method, system and apparatus for preparing, linking, filing, accessing, retrieving, transmitting and auditing of said documents such as medical testing related documents of litigants and in particular linking identity of legal authority mandating testing and individual mandated by court to be tested with test specimen and resulting medical records of tests performed.

## Background Art

Documents and reports whether in written or digital format are prepared, stored and retrieved in order to perform the daily functions of commerce and social life. Examples of such documents include legal paperwork such

as contracts, wills, proceedings, judgments, orders and the like. Consistent with sound legal practice, it is necessary for judges, courts and attorneys to prepare, record and review a wide variety of documents including consultations with experts, outlines of questions, client interviews, depositions, notes and copies, research regarding legal issues, case law relative to legal issues of a case and the like. Furthermore, the court has need to order actions such as mandated drug testing and the like and to prepare and archive such orders and to receive reports of such orders and testing and to archive and store for later reference such test reports and many other types of documents such as court orders, trial proceedings, evidence lists, jury instructions and the like. The rapid, efficient and accurate preparation, linking, filing, accessing, sorting, retrieving, transmitting and auditing of said reports and documents is important to the secure, efficient, and just functioning of commerce such as the judicial courts. Several systems are known to conclusively link such documents with the identity of the humans involved with and authorized to access said legal documents. Examples of systems for accomplishing this include US Patent No. 5,444,615 Attorney Terminal Having Outline Preparation Capabilities for Managing Trial Proceedings filed 20 October 1994 which prior art is hereby incorporated herein by reference.

It is further necessary to secure said documents from unauthorized access and alteration. Current systems however are cumbersome and often require manual retrieval with difficulties in manner of search such as lost documents and files misplaced. Files may be lost and important documents may not be retrieved in a timely manner. Furthermore, current systems are linked often to the name of a litigant or judge and such names are often miswritten or misspelled or similar in sound leading to problems in filing and retrieval of records. There are presently a large number of personal identification systems that directly identify an individual through some portion of the anatomy, e.g. fingerprints, iris of the eye, x-rays, etc. However, none of these systems can be conveniently linked to document identification, sorting or retrieval systems.

Legal documents may comprise court orders, trial proceedings, evidence lists, jury instructions and the like, etc. Known methods for identifying and linking a litigant's name, social security number and other information with the legal documents and reports include linked computer file databases and physically associating litigant identifying data to the printed, numbered document or report. However, associating documents and reports with the wrong litigant is still common in the legal practice.

The liability and inconvenience for the litigant and the legal practitioner and court as a result of

associating said documents and data with the wrong litigant can be considerable. Liability can include inefficiency and time consuming mistakes in applying court orders, unnecessary proceedings, repeated searches for lost documents, psychological distress on the part of the litigant and legal recourse against the legal practitioner.

Given these and other shortcomings in the art, the need for certain new and useful improvements is evident. Accordingly, it would be highly desirable to provide improved methods, systems and apparatus for preparing, linking, filing, accessing, sorting, retrieving, transmitting and auditing of legal documents and in particular linking said legal documents to identity of litigant or other individual with whom the documents pertain and for whom access is appropriately facilitated.

It is an object of the present invention to provide new and improved methods, systems, and apparatus for filing and retrieving documents and reports using two dimensional bar code technology and biometrics.

## Disclosure of the Invention

The above problems and others are at least partially solved and the above purposes and others are realized in improved methods, systems and apparatus for preparing, linking, filing, accessing, sorting, retrieving, transmitting and auditing legal data and in particular for linking litigant identity with his or her drug testing studies and associated linkage of judge ordering said mandated drug testing. In a particular embodiment the invention provides a method of linking medical information with the identity of a litigant supplying the medical specimen, comprising the steps of recording the court order linked to the judge issuing the order, collecting biometric data indicative of the identity of the judge issuing the order, collecting biometric data indicative of the identity of the litigant as registration of litigant for whom drug testing is ordered, collecting digital photograph of the face of the litigant as verification of appearance of litigant for whom drug testing is ordered, re-collecting litigant biometric data at the collection point of collecting a medical specimen from the litigant suitable for drug testing for example blood, urine, hair or sweat sample using the procedure of wearable or swipe patch specimen of PharmChek of California or Securetec of Germany, and linking the biometric data of both the judge and the litigant with the digital photograph of

the litigant and the medical information gained from testing the specimen to form a document expressing the medical information and the litigant identity and judge biometric data and linked to the litigant digital photo. The method may further include the step of storing the record to a data base of a computer in the form of a data file. To ensure the record concerns a specific litigant, the method may further include the steps of re-collecting a digital photo indicative of the appearance of the litigant at the time of specimen donation and comparing the re-collected digital photo with the digital photograph of the litigant at registration. To ensure the record concerns a specific litigant, the method may further include the steps of re-collecting biometric data indicative of the identity of the litigant and comparing the re-collected biometric data with the litigant biometric data of the data file. A means of comparing the biometric data are described in a preferred embodiment of computerized means using low density encoding methods such as smart cards or specifically a two-dimensional bar code.

Briefly, to achieve the desired objects of the instant invention in accordance with a preferred embodiment thereof, provided is a method for the authorization of documents comprising the steps of preparing a record for future reference by authorized personnel including providing a document including data pertaining to an individual, collecting biometric data

from the individual and forming a bar code including the biometric data, attaching the bar code to the document, and storing the document and attached bar code; and authenticating the document and attached bar code upon removal from storage by collecting current biometric data from a person allegedly the individual, comparing the current biometric data to the biometric data included in the bar code, and confirming by a positive comparison that the person and the individual are identical and that the document pertains to the person and the individual, and authorizing the removal of the document from storage. It should be understood that the term 'authorization' as used throughout this disclosure includes verification of documents and persons to whom they pertain as well as authority to access the documents. Also, the term 'bar code' is defined herein to mean any of various two-dimensional bar codes, cross-hatched codes, bar codes with a non-copy type of background, and bar codes that are readable by either optical, magnetic, or any other of the well known means.

To further achieve the desired objects of the instant invention in accordance with a preferred embodiment thereof, provided is a method for the authorization of documents comprising the steps of preparing a record for future reference by authorized personnel including providing a document, collecting biometric data from an individual requesting authority to become an authorized person to access the document,

forming a bar code including the biometric data from the individual, attaching the bar code to the document, and storing the document and attached bar code; authorizing access to the document by collecting current biometric data from a person requesting access to the document, comparing the current biometric data to the bar code attached to the document, and confirming by a positive comparison that the person requesting access and the individual are identical and that the person has authority to access the document.

To further achieve the desired objects of the instant invention in accordance with a preferred embodiment thereof, provided is a method for the authorization of documents comprising the steps of preparing a record for future reference by authorized personnel including providing a document including data pertaining to an individual, collecting biometric data from the individual and forming a bar code including the biometric data, attaching the bar code to the document, and storing the document and attached bar code; authenticating the document and attached bar code by collecting current biometric data from a person allegedly the individual, comparing the current biometric data to the biometric data included in the bar code, and confirming that the person and the individual are identical and that the document pertains to the person and the individual; preparing the document for future access by authorized personnel including

collecting biometric data from an individual requesting authority to become an authorized person to access the document, forming a bar code including the biometric data from the individual requesting authority, attaching the bar code to the document, and storing the document and attached bar code; and authorizing access to the document by collecting current biometric data from a person requesting access to the document, comparing the current biometric data to the bar code attached to the document, and confirming that the person requesting access and the individual are identical and that the person has authority to access the document.

Briefly, to achieve the desired objects of the instant invention in accordance with a preferred embodiment thereof, provided is apparatus for authorization to access documents including the document to be accessed, a bar code including biometric data from an authorized individual attached to the document, apparatus for collecting current biometric data from a person requesting access to the document, and comparing means for comparing the current biometric data to the bar code attached to the document to confirm by a positive comparison that the person requesting access and the authorized individual are identical and that the person has authority to access the document.

The invention may also provide a system for linking legal information with the identity of a litigant who is principally associated as the subject of the legal

information comprising first apparatus for collecting biometric data indicative of the identity of the litigant, second apparatus for collecting digital photograph from the litigant, and third apparatus for linking the biometric data with the digital photograph and for forming and storing a document expressing the legal information and the biometric data and the digital photograph. The first apparatus normally comprises a biometric scanner, and the third apparatus normally comprises a computer coupled or linked with the first and second apparatus in data communication.

## Brief Description of the Drawings

The foregoing and further and more specific objects and advantages of the instant invention will become readily apparent to those skilled in the art from the following detailed description thereof taken in conjunction with the drawings in which:

FIGS. 1 through 4 illustrate a simplified diagram of a verification system and method of using same in accordance with the present invention;

FIG. 5 illustrates a flowchart of method steps for legal data collection, recording, updating and data access using biometric data with suitable judicial review;

FIG. 6 is a block diagram illustrating the steps involved in auditing the database using biometric codes;

FIG. 7 is an illustration of a clerk confirming litigant identity as litigant consents to registration of litigant biometric;

FIG. 8 illustrates an attorney surrogate copying litigant drug testing file on digital copier using iris code authorization by surrogate;

FIG. 9 illustrates an attorney accessing litigant file over encrypted transmission line;

FIG. 10 is an illustration of the authorization of a judge to transmit a legal document to a website over the Internet using biometric code authorization and encrypted data transmission;

FIG. 11 is an illustration of the fax apparatus in use wherein the sender enters biometric code and the receiver optionally also enters biometric code on linked biometric scanners;

FIG. 12 is a diagram of the standard registration station of the instant invention in one embodiment; and

FIGS. 13- 23 illustrate various interrogations and instructions descriptive of the use of the instant invention in drug testing a litigant, as they appear in the system.

## Best Modes for Carrying Out the Invention

Ensuing embodiments of the invention comprise new and improved methods, systems and apparatus for accurately linking human subject biometric data with

documents pertaining to him or her as subject or to which access is appropriate for example legal documents and reports with respect to the subject of court mandated testing and with respect to access to results of such court mandated testing. Further, the new and improved methods, systems and apparatus include means for verifying the accuracy to the users during each use. A wide variety of legal documents and reports containing information concerning legal matters such as court orders or legal proceedings or subjects, whether stored in a computer data base or in hard copy form, may be classified under the ambit of legal documents. Furthermore, linking the biometric data of a human subject with his or her pertinent legal documents in accordance with the invention prevents mismatching legal documents with the wrong litigant or judge. Throughout this disclosure the terms "biometric" and "biometric data" are defined as data collected by biometric devices or systems, which are those that collect and process data files consisting of data representing a measurement of some particular aspect of a human body or body function, such as an iris scan, fingerprint, handwriting, facial recognition, etc. The biometric device or system functions by registering an individual and taking an initial biometric reading. The device or system then takes a second reading and performs a match of the second reading to the initial reading to verify that they represent the same individual. One of the

limiting factors to an expanded use of biometric devices or systems is the lack of sufficient feedback to the user which can satisfy that user of the accuracy achieved using the biometric method of identification.

Typically a biometric device or system has an admitted error rate that is often expressed as false accept and false reject statistics. Such error rates admit a problem occurs on occasion, albeit rare, and that the biometric device or system may, for example, incorrectly match a biometric reading of one individual to a data file of another individual (false accept) or alternatively not match any data file despite the fact that the person is registered within the system (false reject). The implication of such errors depends on the application that the system is supposed to be performing. For example, denying physical access to a job site based on a false reject of a biometric reading of a user who is authorized to enter that job site is a relatively minor problem since that person can merely reapply another biometric reading and likely gain access. A more severe consequence of a false accept by such a biometric system applied to monitoring site access might be permitting access to someone not authorized, for example to a bank vault.

Some applications of biometric systems involve such sensitive matters that proper functioning can tolerate no errors. One example is the use of biometric systems to deliver health test data such as medical reports. In

such cases the use of biometric devices or systems which have even a rare false accept or reject of data files is problematic. Furthermore, the user of such an application might well be aware of the sensitivity of the application. In such circumstances and in accordance with the present invention, the user of a biometric identification system applied to a very sensitive application, can have confidence that the proper biometric match has occurred because the biometric systems described below optionally provide a feedback giving the user evidence of a proper match. Furthermore, where governmental oversight bodies, such as the FDA, are asked to accept the match of important data, such as medical data, to a user through a biometric system, there is a need to provide some means of verifying, double-checking, or auditing of a correct match. Thus, herein disclosed is a verification or feedback system or means that verifies to a user or observer that a biometric device or system has functioned properly. The verification or feedback system or means provides a feedback signal that can take the form of a visual feedback and in such format should present to the user an image which, by the display of such image, conveys confidence that the biometric system has performed properly.

In a preferred embodiment of the verification system, the user registers a first biometric, such as a right eye scan, in a standard manner, for example by

providing an iris scan using commercially available equipment from IriScan of Marlton, New Jersey. The system has a digital camera linked in it and the user, while giving the iris scan for registration, has his or her full face photo taken, preferably with a digital camera. The digital image data is then entered into a computer in the verification system. The same user then registers a scan of the left eye and the right and left iris scans data files are linked in the computer of the system to the digital image data from the photograph. Label data, in the form of bar codes, etc. (to be described in more detail presently) can be generated by the computer of the system as needed.

At any later time, the user returns and wishes to use the biometric system, for example to access medical test results from analysis of his specimens which were submitted anonymously to the laboratory and identified only by label data linked to the biometric data of the user. In the instant embodiment, the user performs a right eye scan and the biometric system matches the correct data file of the right eye biometric. This match also identifies the photo digital data linked by the computer in the file. In this embodiment the user's image is split into segments which are approximately every other segment of the full face photo to be displayed on a monitor.

The user then scans his or her left eye and the biometric system correctly matches the left eye

biometric data to the user's stored file. The left eye biometric data stored in the user's file is also linked to the full face photo, which is similarly divided into alternate segments. This time the alternate segments chosen for display are the other half of the full face photo displayed in response to the right eye scan. The computer program is written to instruct the biometric system to display the two alternately segmented images together, thus forming a complete full face photo which is the image of the user. The user, seeing his or her image on the monitor, is able to recognize the photo and know that both biometric matches were correct. The system can then be activated to display the desired medical data such as test results. In some instances it may be desirable that the photo not identify the user and in such cases a personal photo known to the user can be scanned into the user's file in the computer memory as a substitute. For example, a family picnic or a photo of a pet could be used. The user would recognize the photo when composited on the monitor through right and left eye scan matches.

The verification system is illustrated and disclosed in more detail with reference to FIGS. 1 through 4. Referring specifically to FIG. 1, a user 30 inputs a biometric reading, which in this specific example is a right eye iris scan, using an iris scanner 31 attached to a computer 33 having a monitor 34. Iris scanner 31 can be any one of several commercially

available iris scanners, such as one from LG Technologies of Korea or IriScan Corporation of Marlton, New Jersey. Immediately after the right eye iris scan, user 30 turns to a digital camera 35, which is also linked to computer 33, and an operator 37 pushes a button on digital camera 35 causing digital camera 35 to take a full face picture of user 30. User 30 then turns back to iris scanner 31 and registers a left eye iris scan. Software in computer 33 splits the full face image of user 30 from digital camera 35 into two partial images, typically by alternating segments (e.g. each partial image includes four alternate 45° segments) or by radial division of the image according to a center point at the bridge of the nose and proceeding according to the compass beginning at zero degrees and alternating every other 15 degrees. Two partial images can also be formed by alternating a specific number of horizontal sweep lines in monitor 34. For example every other five sweep lines could be in alternate images. Thus, sweep lines 1 - 5, 11 - 16, etc. would be in the first partial image and sweep lies 6 - 10, 17 - 21, etc. would compose the second partial image.

The portion of the facial photo of user 30 to be assigned to the right eye data file is referred to as the first partial image and the portion of the facial photo to be assigned to the left eye is referred to as the second partial image. The right eye iris scan is processed by computer 33 and is placed in a file. The

file also has stored therein the first partial image, which is linked to the right iris scan. Similarly, the left iris scan is processed by computer 33 and is placed in the file and linked to the second partial scan, which is also stored in the file. Further, any sensitive data of user 30, such as HIV medical test results, is stored in the file and the file is locked so that it can be accessed only by authorized personnel.

Referring additionally to FIG. 2, user 30 (at some later time) returns to iris scanner 31 for the purpose of identification and access to his sensitive data file under his biometric linked file in computer 33. In this instance, user 30 brings with him a second person 38 for whom he wishes to display the sensitive data on computer monitor 34. User 30 inputs his right eye iris scan by way of iris scanner 31. The iris scan is processed and matched correctly to the database item corresponding to the right eye of user 30. This match is correct and causes computer 33 to display the first partial image designated 40, of user 30, which in this specific embodiment includes alternate arcuate segments from zero to 45 degrees, 90 to 135 degrees, 180 to 225 degrees, and 270 to 315 degrees.

Referring additionally to FIG. 3, user 30 inputs a second biometric reading, in this specific example the left eye iris scan using iris scanner 31. The left eye iris scan is correctly processed by computer 33 and correctly linked to the database item corresponding to

the left eye iris scan of user 30. This match is correct and causes computer 33 to display the second partial image designated 41, of user 30, which in this specific embodiment includes alternate arcuate segments from 45 to 90 degrees, 135 to 180 degrees, 225 to 270 degrees, and 315 to 360 degrees. The superimposing of the first and second partial images 40 and 41 on monitor 34 produces a full face image of user 30.

Digital camera 35 linked to the verification system is again signaled or activated by operator 37 and takes a second full face photo 42 of user 30. Computer 33 receives the second digital image data and links that data to a transaction record which also includes the details of which iris files were matched and composite photo 40/41 produced by the right and left iris matches. Computer 33 optionally displays the second transaction facial image 42 side by side (see FIG. 4) with composite image 40/41 produced by the match of the right and left iris scans of user 30. A record of the two images is placed in the transaction data file. These two images side by side constitute a record of the transaction which is auditable.

In the case where an incorrect match is made, for example, to a right eye iris scan file, computer 33 will display on monitor 34 a partial image that is of another individual than the true identity of user 30. Even where the left eye iris scan is correctly matched, the composite image will not be of user 30 but rather of

another or a distortion such as a composite of two different individuals. Thus, the method, system, and apparatus herein disclosed permit user 30 and observer 38 to see that the match has been in error and that a rescan is required in order to find a correct match. As will be understood upon studying the various embodiments disclosed below, the verification system described above can optionally be incorporated in any of the embodiments disclosed below or can be a system which stands alone.

In a specific example of the present invention, verification of a patients identity occurs as the litigant proceeds to the laboratory for donation of a specimen for drug testing. Laboratory personnel recollect biometric data from the litigant from the same part of anatomy as used to register the litigant at the court, for example the same eye iris scan or the same finger scan. The computer retrieves the registration data by comparing the input of litigant biometric data at the laboratory to the litigant biometric data recorded in the computer file at the time of litigant registration. The computer, after matching the biometric data, retrieves the digital image of the litigant and displays the litigant image on the monitor of the computer of the laboratory. The laboratory technician, as one means to verify identity of the litigant, optionally compares the image on the monitor to the image of the litigant presenting himself in the laboratory. Furthermore, the laboratory technician may

ask for additional identification from the litigant such as driver's license to compare to the demographic data stored in the computer file linked to the litigant biometric. Optionally, the technician can also compare the monitor image of the litigant to the litigants image on the demographic card. Once the comparison verifies the identity of the litigant the computer signals the bar code printer to print a two-dimensional bar code sticker to be placed on the specimen container which contains the specimen donated by the litigant, see for example US Patent No. 5,876,926, entitled Method. Apparatus and System for Verification of Human Medical Data, filed 6 August 1997, and incorporated herein by reference.

The biometric data of the ordering judge can be linked in the computer to a data file of the litigant and order for drug testing. The computer and its software and printer can be easily configured to print a hard copy of the results of the drug test having a two-dimensional bar code of the biometric data of the litigant that the drug testing study concerns. Certainly the litigants name, address, social security number and other information may also be linked to, and printed on, the hard copy of the litigants drug testing study and the computer data file of the litigant linked to the digital photos of the litigant at registration and the digital photos of the litigant taken at the laboratory during specimen donation.

In accordance with the present method, when a judge orders a drug test on a litigant, the judge is granted access to the resulting data file via alphanumeric access code on computer keyboard or optionally via the judge registering his biometric code as access code and matching that registered code during access or preferably by the judge scanning the litigant bar code from litigant file. Typically the judge assigns a legal clerk to review the drug testing of each litigant mandated to submit to drug testing. The clerk has access based on an access code which the clerk inputs into the keyboard or optionally the clerk registers his biometric code for access authority. The data files can be accessed from the computer and viewed on a computer screen, or printed from the computer as a report bearing the two dimensional bar code encoding the biometric code of the litigant.

Another embodiment of the invention contemplates a method, system and apparatus for allowing a litigant to re-enter his biometric data at a later date after, for instance, completing the series of court mandated drug testing. This may be accomplished by scanning the two-dimensional bar code printed on the litigant's drug testing reports and file in the court records and then scanning the litigant biometric data, wherein a computer receives both bar code data and biometric data and compares them to confirm that the drug testing reports represent data regarding the same litigant. This

process can be accomplished by utilizing a bar code printer attached to the laboratory computer which relates the biometric code of the specimen sample and then prints the corresponding two dimensional bar code on the report. The biometric scanner linked to a computer located at the court having access to the laboratory data files optionally by ISDN line or modem is linked to the data system containing the drug testing reports and corresponding biometric data. This comparison provides the legal clerk or technician or judge with an exemplary means of verifying that the identity of the litigant matches the identity of the individual tested by the laboratory in accordance with the court order.

In a preferred embodiment a rendering of the digitized iris data, such as a two-dimensional bar code of litigant, can be placed on the master file, each individual laboratory report and in computer linked files for electronic comparison and printing. Sorting of reports for filing in a master file is then envisioned by scanning of the two dimensional bar code on the report and then scanning of the two dimensional bar code on the file cover and then placing the report into the file where the computer confirms a match, indicating that the biometric code of the identity of the file matches the biometric code identifying the donor of the specimen used for testing and reported on the test report.

In one embodiment, the present method and apparatus includes the use of an encryption for data files and optionally a network of linked computers such as linked to the Internet. The system uses, as identification for a person, a biometric measurement or data of a portion of the anatomy of that person. Biometric measurements or data can include fingerprint or iris of the eye patterns, or measurement of a function of the anatomy of said person such as signature or voice recognition or voice print, etc. The biometric measurements or data are then encoded for storage in a computer database or other storage medium. Encoding typically takes place during the process of obtaining the biometric data. The use of the invention for the authorizing attorney is similar to the system for physician authorization as disclosed in PCT/US 99/08120 entitled Method, System and Apparatus for Biometric Identification filed 14 April 1999, invented by the same inventor as the instant invention, owned by the same entity, and incorporated herein by reference.

As a preferred embodiment, the use of an iris scan is herein disclosed wherein each attorney within a geographic region or jurisdiction, such as within one state, authorized to access data computer files of the system computer, is registered by his or her iris code created from an image of his or her iris. This registration can be made using, for example, an iris scanner such as produced by IriScan of Marlton, New

Jersey or the auto-focus iris scanner of LG Technologies of Korea. The iris scan measurement is encoded and filed in a computerized database optionally within a single database of a central computer. The attorney when authorizing formation of a data file for a litigant or client will have in his office an iris scanner and will instruct the litigant or client to enter iris data, typically from the right eye, into the scanner. This scanner is linked to the central database of the computer system of the attorney. The litigant or client encoded iris scan data and the attorney encoded iris scan data are thus linked in a data file which optionally includes further specifications such as time, date, legal notes, court orders, court mandated drug testing data and the like. It will be understood that while an iris scan is used for purposes of example in this specific embodiment, other biometric measurements or data can be employed and encoded for storage into the computer data base.

When the litigant or client visits the attorney to have a second interview or legal consultation, the computer searches the database of iris codes of litigants or clients who are currently in the attorney database. When a match of encoded iris data occurs, the data is displayed to the attorney or office staff authorized to view the data. In the circumstance where a litigant has recently consulted with and chosen to employ a new or other attorney and where the litigant

has previously registered data files with a first attorney and where the new attorney and the first attorney each have a computer system in conformity with the instant invention, then at the new attorneys office the litigant is enabled to enter his biometric code into the network of computers linking the first attorneys computer to the new attorneys computer. In this manner the litigant is enabled to transfer litigant data files from the custody of the first attorney to the custody of the new attorney. Optionally the data files are encrypted for transmission and optionally the data files include video testimony files and audio files as well as documents.

In another embodiment, the computer recognizes that the litigant may bear a card which has the litigant bar code as representing the iris data of the litigant. The new attorney office staff may ask the litigant to sign a consent to allow the new attorney office staff to access the data files stored in another computer linked to the new attorney computer. The scan of the bar code by the new attorneys office staff is matched to the iris scan of the litigant obtained at the time of the consent thus confirming the litigant bar code refers to the litigant himself and not another person. The computer then is prompted to search the data base of registered litigants in relation the bar code identification. The computer displays the name of the litigant and the name of any attorney or judge or legal proceedings linked to the

litigant name in the computer. The attorney is thus alerted through consent from the client or litigant who has sought the attorney services of any prior legal consultations and action and proceedings including the names of previous attorneys, judges, and the like who have been connected with the litigant or client in the past. Where the instant invention is connected with a website of the Internet that registers clients linked to attorney names then the data includes multi-state and international data as appropriate. Other data optionally envisioned to be linked to the litigant data file include credit report and indication as to whether the previous attorney has or has not been paid for services rendered by the previous attorney to the litigant.

It is envisioned that the litigant optionally will have a digital photograph taken upon registration of biometric data. In this regard art by the same inventor and owned by the same entity as the instant invention is US Patent Application number 60/109,287 entitled Method, System and Apparatus for Feedback of Biometric System Function, filed 20 November 1998 and which is incorporated herein by reference. This digital photograph is optionally envisioned to be taken by a standard digital camera linked to the computer of the system. The digital photograph is optionally linked to the data file of the litigant (as shown and described below in conjunction with the attached FIGS. 13 - 23).

The litigant is envisioned to have a second digital photograph taken at a later date such as the visit of the litigant to the laboratory to donate a specimen for drug testing in compliance with a court order. The digital photographs are envisioned to be linked in the computer data file of the computer and form an audit trail of litigant activities and appearance at specified date and times. Access to the litigant digital photograph data and linked time/date information is envisioned to be controlled in a manner similar to the herein described data access method.

Thus, a biometric access event to a unified database of legal services clients and attorneys is envisioned herein whereby an attempt to access data is recorded in a manner similar to the manner in which a litigant is registered. The individual who attempts to access data can be photographed digitally and submit biometric data identifying the person attempting access. The attempt if successful results in a record in the computer that records the identity of the individual who accessed a data file linked to the data file accessed. The access event record includes the biometric data and optionally the digital photograph of the person who accessed the data. The record of data access and attempted data access is thus able to be audited. The audit search is envisioned to be based on criteria of search. For example, a computer search can be performed for all files accessed, or attempted to be accessed, by

a particular individual within the past 12 months. Such a search of the database is enabled through the use of scan of a bar code that encodes the iris data matching for example a particular attorney. The clerk of the court can scan the bar code and the computer retrieves any matches and prints an audit listing the dates of access of files and the number of each file and optionally the name of litigants linked to the files.

It is envisioned that an attorney will wish his paralegal personnel for example to have authority to access certain files in the hierarchy of files in the attorney data base. Similarly it is envisioned that a judge will wish to have clerks and certain surrogates to have authority to access certain files in the court data base. The attorney or judge in the scope of the instant invention will be enabled to register surrogates. This is in a manner similar to the physician registering surrogates as disclosed in the art herein cited as PCT/US 99/08120 by the same inventor as the instant invention and owned by the same entity and herein incorporated by reference. Thus those surrogates authorized to carry out data input function for, or at the instruction of, a particular judge are registered by encoded surrogate iris data linked to said judge's iris code data file in the computer. The system in operation optionally requires the surrogate iris data to be re-entered in order to allow the computer to match the code against the data base of iris codes and where a match is

made identifying the surrogate as authorized to access a certain file linked to the judge then the surrogate is allowed to access a certain data file for the judge. Similarly if authority is recorded in the computer for the surrogate to alter the judge's linked files, then the surrogate may alter a file in response to instructions from the judge for whom the surrogate is acting. The activities of the surrogate are then recorded by surrogate biometric and can be audited in accordance with the instant invention. It is also envisioned that a data base of surrogates for the legal profession can be maintained optionally via a website of the Internet. Such data base is envisioned to be a data base that links the paralegal biometric to the paralegal work history in a manner that allows an attorney authorized by the paralegal to access the work history over a computer linked to the website.

Turning now to FIG. 5, the instant invention is illustrated as pertaining to a judge A who issues an order 101 in relationship to drug testing mandated for litigant X. Judge order 101 is recorded in the database of the computer linked to a judge A biometric. The judge has several assistants who serve as surrogate for judge A. One such surrogate registers litigant X's biometric at step 103 and optionally records litigant X's digital photograph which biometric and digital photo are linked in the database to the file containing the judge A order for drug testing of litigant X. At step

102 the bar code printer linked to the court computer prints a bar code sticker which sticker encodes the iris code of the litigant X. At step 102 this bar code is placed by the surrogate of judge A on the litigant X paper file which file is then given by the surrogate of judge A to judge A.

Litigant X is represented by attorney Y whose biometric is also registered in the court computer database. For purposes of illustration Attorney Y has been retained by litigant X. Attorney Ys biometric is thus linked to the litigant X data file as the attorney authorized to access the litigant X data file at step 105. Also Attorney Y has registered one of his surrogates, surrogate W, as authorized to access the litigant X data file in the name of Attorney Y. At step 107 surrogate W accesses the litigant X data file. In accordance with the instructions from Attorney Y entered by Attorney Y, using a keyboard linked to the Attorney Y computer, into the data file of the Attorney Y office linked computer in relation to the litigant X file, surrogate W arranges the visit of litigant X to the laboratory. In accordance with the judge A order, attorney Y through surrogate W telephones litigant X and advises litigant X to proceed to the laboratory for testing. Litigant X upon arriving at the laboratory is re-scanned at step 111 for biometric, in this example the iris code of the same eye as used for registration in the court computer at step 103. The litigants iris

code is matched by the computer at the laboratory which is linked to the database of biometric codes of litigants as recorded in the court computer. The laboratory matches litigant Xs biometric, retrieves the demographic data of litigant X, and displays the data on the laboratory computer monitor for the use of the laboratory staff in verifying the identity of litigant Xs demographic data optionally including litigant Xs name, driver's license # and the like as well as displaying the digital photograph of litigant X as recorded at step 103.

After the laboratory staff person verifies that litigant X is the same person as the person registered as litigant X in the court computer, litigant X is re-photographed by the digital camera linked to the laboratory computer. The digital photo of litigant X in the laboratory is linked to the data file of litigant X in the court computer and to the data file of the laboratory computer for use in verifying presence and identity of litigant X including for later audit purposes. The audit function of the system is further detailed below. At step 115 litigant X donates a specimen for drug testing and said specimen container is labeled by a two dimensional bar code which encodes the biometric of litigant X in accordance with the prior art cited above. The laboratory performs the test on the specimen and links the results to the data file of litigant X in the laboratory computer at step 117.

After the test is verified as correct by a laboratory supervisor whose biometric is optionally recorded marking professional judgment of satisfactory results for litigant Xs test performance, then at step 117 the results are sent to the court computer by modem line or similar communications means and received by a court computer linked to litigant X data file. The results are reviewed by the judge at step 121, wherein the judge uses a bar code scanner linked to the court computer to scan the two dimensional bar code sticker on the file page of litigant Xs paper file in the judges chamber. This scan retrieves the data file of litigant X from the computer, optionally only after judge A also enters his biometric code by iris scan of his right eye as authorization to access the litigant X data file and associated digital photos of litigant by date/time. The judge dictates an additional order for the file and at step 123 a surrogate of judge A enters the file and at step 125 adds data in correspondence to the judge A amended order.

At step 127 attorney Y's surrogate W accesses litigant Xs data file and reads judge A's amended order. Surrogate W, at step 128, informs Attorney Y of the amended order and at step 129 Attorney Y instructs surrogate W to inform litigant X that the judge has entered an amended order. At step 129 surrogate W records in the Attorney Y computer data file of litigant X the action instructed by Attorney Y. At step 133

attorney Y's billing instructions for billing Attorney Y services rendered to litigant X are given to surrogate W and said billing of litigant X is recorded by surrogate W and linked to the data file of litigant X. The billing is sent to litigant X and upon payment a recording of such payment is made into the data file. Further instructions from litigant X to Attorney Y are recorded in step 135. Attorney Y in carrying out said additional instructions prepares a brief for litigant X and said brief is linked to litigant Xs file in the Attorney Y database. At step 139 Attorney Y authorizes by biometric code the transfer of the brief to judge A, which brief is transferred via fax **or e-mail**. A copy of the brief is made by surrogate W using a copier which requires surrogate W to first identify herself via her iris code to the copier. The identity of surrogate W is recorded in a bar code on the copy of the brief as printed by a printer linked to Attorney Ys computer. The copy of the brief is given by surrogate W to litigant X at the instruction of Attorney Y.

Turning now to FIG. 6, illustrated is the database of FIG. 5 including legal data linked to biometric codes of various individuals including judges biometric data, the judge surrogates biometric data, attorney Ys biometric data and client Xs biometric data and surrogate Ws biometric data. For purposes of illustration of audit function of this database step 201 represents an inquiry by judge A requesting to see all

judge A linked files for a twelve month period specified by judge A on keyboard entry of computer. The data files are summarized for judge A on the screen of the computer monitor in judge As chamber at step 203. Judge A makes a note into the computer file at step 205. Optionally, Judge A may wish to transfer a file to another judge. Judge A sends the file electronically using the judge A biometric code at step 207 and, optionally, a surrogate of the receiving judge acknowledges the transfer by input of a surrogate biometric code.

At step 209, an attorney inquiry is illustrated wherein an attorney registered by biometric code accesses a record of all files linked to one of his law partners wherein the law partner has previously registered said attorney as authorized by the partner to access the partner's linked data files. At step 211 the data files are displayed and at step 213 the attorney makes an entry into one data file. This action is recorded as to time and date and individual making the entry via the biometric of the attorney making the entry. The file change is later verified at step 215 by said partner attorney using his or her own biometric.

At step 217 a litigant is able to access his own data file or preferably certain aspects of his file as judge A determines. The litigant uses his own biometric code, which optionally may include more than one type of biometric as for example an iris code and a fingerprint

scan. This entry is optionally further verified by digital photo at the time of entry by litigant into the file and this digital photo is recorded and linked to the data file as evidence that the litigant opened the file at that time. At step 219 the data file is displayed. At step 221 the litigant is enabled to make a copy using his biometric and a printer of the system. At step 223 the copy is verified by printer recording on the paper of the copy printed the biometric of the litigant and optionally the time and date of printing. Optionally this printing of a bar code onto the copy is via a transparent label or optionally via a black line having infrared readable bar code of litigant.

At step 225 a surrogate of judge A enters a surrogate biometric and requests to view another judges records for whom the surrogate is not registered as authorized to access files. The computer in matching this surrogates biometric finds that this surrogate is not authorized to access the records requested. This event is recorded by the computer and at step 227 an e-mail is sent to the judge whose records were attempted to be accessed indicating the attempt at unauthorized access and the identity of the surrogate so attempting access. Furthermore, the surrogate thus making an unauthorized attempt is optionally identified to all nodes of the system and prevented further computer data activities. The data base privileges of this surrogate are temporally changed by automatic algorithm of the

computer to prevent any further access to any files in the database. The privileges can be re-instated by the manager of the database upon satisfactory explanation of the unauthorized access attempt by the surrogate, for example an unintentional error in the keyboard entry of the wrong judges name. At step 229 the manager reinstates the surrogate privileges.

At step 251 a request to copy files is received by the database computer from a website linked computer. The request is accompanied by the biometric code of the litigant whose file is requested to be copied. The computer compares the code to the biometric code in the database for that litigant. At step 253 the computer verifies a match and at step 255 the computer authorizes a surrogate of the judge supervising that case to make a copy. At step 257 the surrogate mails the copy to the requesting attorney representing litigant. At step 259 a telephone request is received to send records. The request is accompanied by a biometric code from a cellular telephone linked biometric scanner. The computer matches the biometric code to a judge in the database at step 261. The computer at step 263 then reviews privileges of the judge to determine whether the judge is authorized to view the data file. The computer after verifying authorization then sends by e-mail the requested data file to the e-mail address provided by the requesting judge in the telephone request.

At step 265 the computer performs a monthly automatic audit of activity. At step 267 the report of activity, which optionally includes a number of cases assigned to each judge and a number of cases of specific categories and disposition of cases and the like is collated and filed in the database. At step 269 the chief judge inputs his or her biometric as a request to see the report. At step 271 the computer verifies the chief judges identity and authorization to see the report and prints a copy of the report on the printer of the chief judges chamber. A record of the request and of the transaction is kept in the database. Similar office data reports are envisioned from each attorneys office computer and optionally the law practice computer is prompted each month to print out a series of reports. These reports provide the supervising attorney or managing partner with oversight data regarding the work activities of each attorney or surrogate registered in the system. Similarly, the instant embodiment is envisioned to produce reports, where authorized to do so, which reports can be accessed by the appropriate State Board or judge with oversight responsibility of the data regarding the legal activities of a particular litigant or attorney.

Turning now to FIG. 7, illustrated is the registration of a litigant 312 by a surrogate 314 wherein litigant 312 supplies a fingerprint scan using scanner 301 and also provides a digital photo via a

digital camera 305 linked to the system. Litigant 312 may also sign a standard consent form. A keyboard 303 of a computer 311 is used by litigant to enter demographics and the printer prints an identification card 322 bearing the demographics and the two dimensional bar codes representing litigant 312 as bar code 325 and the attorney as bar code 323. The surrogate is confirming the data entry of litigant 312 by input of surrogate fingerprint code and iris code on scanners 319 and 317, respectively.

Turning now to FIG. 8, illustrated is the use of a specialized digital copier 494 linked to the system of a computer network 495 via a link 496. Copier 494 has attached a biometric scanner 498. Copier 494 performs copies of documents (e.g. document 492) in response to identification of an individual 499 operating the copier using a data base of biometric readings and matching the input of the biometric of the operator to the data base. A computer in computer network 495 linked to copier 494 records the input of the biometric of the operator and prints a copy. The copy optionally has encoded into the copy a two dimensional bar code that encodes the biometric of individual 499. This copy is thus able to be scanned later and the identity of the person who operated the copier in making the copy (individual 499 in this instance) can be determined by matching a bar code 493 of document 492 to a data base of biometric codes corresponding to the bar code. Two dimensional

bar code 493 can be visible in normal light or optionally may be printed in the document in a manner that renders bar code 493 difficult to see in normal light but visible to a bar code scanner in ultraviolet or other special light. The biometric data of individual 499 making a copy is optionally recorded into a data file of copier 494. Optionally, copier 494 has a bar code scanner 497 incorporated in such a manner that a document (e.g. document 492) entered into copier 494 to be copied and bearing a two dimensional bar code 493 recognizable to scanner 497, is scanned by scanner 497 permitting the copier computer to record the nature of the document including optionally the identity of the individual whose biometric is encoded into the document. Bar code scanner 497 is optionally mounted in a location corresponding to a standardized location on documents wherein the bar code is placed in a position, such as the top left hand corner of the front page of the document. Optionally, bar code scanner 497 is positioned on a movable mount (not shown) such that scanner 497 can read bar codes placed on other non-standardized locations of the document or alternatively can scan multiple bar codes on a single document. Copier 494 is linked to a computer system or network 495 such that a document bearing a bar code having encoded a number corresponding to the document number can be read. Optionally a computer database file corresponding to that document can be accessed by a computer in computer

network 495 in response to the scan of the document bar code. The contents and layout of the document in file from computer memory is thus compared electronically to the contents and layout of the document as placed on the copier. This comparison is useful to detect any alteration to the document from the original and to record the altered document as it is copied or as described below faxed or alternatively to prevent an altered document from being copied as described below faxed.

Copier 494 optionally records the time and date of the copy and the biometric identity of the individual who is making the copy. Authority to make a copy can be denied if the match of biometric data of the operator links to a biometric not authorized to copy documents or a specific document such as the document bearing a two dimensional bar code. Bar code 493 is utilized for purposes of example and it should be understood that other types of codes (all of which are referred to herein as 'bar codes; for simplicity) can be utilized, such as cross-hatched codes as is well known in the trade wherein the cross hatching is difficult to be copied in the standard copier. The cross hatching code thus has the additional advantage of preventing a copy from passing as an original. The bar code can be designed with red background as an anti-copy protection, as is well known in the art. For example, black characters in red background are readable from the

original by the bar code scanner but the copier typically cannot retain the clarity and readability in the copy as compared to the original. The bar code can alternatively be placed on the back of the document so that the scan can be performed prior to the scan of the document front page so that the computer file can be accessed for comparison. Also, bar codes which are read by optical, magnetic, or other means are envisioned and included in the description. Any attempt to copy said document is optionally recorded.

Turning now to FIG. 9, illustrated is an attorney 414 recently retained by a litigant 412. Litigant 412 is providing an iris code to a scanner 417 linked to the present system wherein said iris code matches the litigants biometric code recorded in the database linked to litigants files. The litigants iris code is sent to a network computer 416 and attorney 414 supplies a fingerprint biometric identification as registration via the consent of litigant 412 as authorized to receive the files of litigant 412. The file demographics are displayed on a monitor of computer 416 and the file is downloaded to computer 416 after a match is verified by attorney 414.

Turning now to FIG. 10, illustrated is a judge 4140 requesting to transmit a document from a computer 7030 to a website using an embodiment incorporating the instant invention. Judge 4140, using a two dimensional bar code scanner 7009, scans a bar code of a litigant

identification card 7011 whose file she wishes to transmit. Judge 4140 also applies her finger to a finger print scanner 7970 and submits to an iris scan by iris scanner 7010 to provide to computer 7030 instant biometric data for authorization relative to judge 4140. Computer 7030 matches the bar code to the litigant biometric linked file and using the authorization provided via fingerprint scanner 7970 and iris scanner 7010 sends the file over the Internet to the destination judge 4140 indicates via a keyboard entry. Here it should be noted that fingerprint scanner 7970 and iris scanner 7010 are illustrated for purposes of example only and either one or both might be utilized, depending upon the amount of security desired, or other biometrics, such as handwriting, voice recognition, etc. might be utilized in addition to or instead of either of the described types.

Turning now to FIG. 11, specialized communication and data handling equipment is linked to a computer network in accordance with the method and system herein disclosed. For example, a specialized fax machine 1717 is linked into a system in accordance with the present invention, wherein a computer linked to fax machine 1717 has a data base of iris codes. In use, fax machine 1717 is given documents for example as printed by copier 494 in FIG. 8 above. The documents bear the two dimensional bar code of the individual who copied the documents. This two dimensional bar code is optionally printed by

copier 494 in a "black out" mode as is well known in the field in which the code is embedded into a black background. The code is not visible readily in normal light but is readable using infrared light using an IR scanner for bar codes, such as scanners manufactured by Nippon Denso of Japan. In this embodiment copier 494 prints a page that contains the encoded iris code of the person who copied the page where that code is not visible to the naked eye due to the embedding of said iris code in a black background. Fax 1717 however is a standard fax machine modified to contain a built in IR bar code scanner (not visible). This scanner is enabled when the copy is entered for faxing to scan the area of the document wherein the black out two dimensional bar code is placed. The placement of the bar code scanner is in such a manner as to read the bar code when placed in the standard location as described for bar code scanner 497 of copier 494. Optionally the fax machine bar code scanner can be coupled with a bar code printer such that a bar code is printed onto the document prior to faxing and such bar code encodes the time of data transfer, date, sender biometric code, recipient biometric code.

Prior to the sending of the fax, the fax machine computer compares the iris code in the black out bar code of the document to the database of iris codes in the fax machine linked computer. Where the iris code of the individual who made the copy matches an iris code in

the data base the computer assesses the privileges of said matching iris code to determine if that person is authorized to provide documents for faxing. Where the person is authorized to provide documents for faxing. the fax machine prompts an operator 1716 of fax machine 1717, who may be a person different from the person who produced the copy, to provide his or her iris to an iris scanner 1707 linked to fax machine 1717. The fax machine linked computer receives the iris code of operator 1716. Where the iris code of operator 1716, who is attempting to fax the copy, matches an iris code in the data base the computer assesses the privileges data in the database of said matching iris code to determine if that person is authorized to fax documents. Where the person is not found to be authorized fax machine 1717 optionally sends a signal such as audible alarm indicating an unauthorized attempt to transmit data. If operator 1716 is authorized to fax documents, fax machine 1717 optionally prompts operator 1716 to input the telephone number of the fax machine to which operator 1716 wishes to fax the document.

In a preferred embodiment a receiving fax machine 1718 is also equipped with an iris scanner 1719 and a bar code reader and printer. Receiving fax machine 1718, upon receiving a prompt from sending fax machine 1717 indicating that sending fax machine 1717 requires iris code identification of a receiving party 1720, receiving fax machine 1718 prompts operator 1720 on the receiving

office staff to attend receiving fax machine 1718. Receiving operator 1720 presents his or her iris to an iris scanner 1719 coupled to receiving fax machine 1718. The receiving operators iris code is transmitted to sending fax machine 1717 and is recorded into the data base of the computer of sending fax machine 1717. Optionally, the linked computer of sending fax machine 1717 compares the receiving operators iris code to the data base of iris codes and where a match is found assesses any linked data to that file which indicates authority to receive fax data from the sender. Where the iris code of receiving operator 1720 is matched to an iris code file indicating receiving operator 1720 is authorized to receive fax transmissions from the sender, sending fax machine 1717 transmits the fax data to receiving fax machine 1718. Optionally the iris code of sending operator 1716 and the iris code of receiving operator 1720 are each recorded in the sending and receiving fax machines 1717 and 1718 and optionally both embedded in the receipt and transmission printed record of the fax transmission. Optionally, the fax machine sending the fax prints onto the fax document the iris codes of the sending and receiving individuals and, optionally, the iris codes are printed as black line IR readable codes. It will of course be understood that various levels of security may be desired and lower levels may require fewer authorizations and/or fewer biometric codes along the path.

Turning now to FIG. 12, illustrated is the standard registration station of one embodiment of the instant invention wherein registrar 801 is seated in front of a keyboard 903 onto which the registrar enters commands. The keyboard is linked to a computer 905 mounted on the base of a table 907 and including a monitor 923 positioned on table 907. Table 907 is mounted on rollers and has a movable top 909 wherein the adjustment of height is controlled by a foot pedal 911. Registrar 801 invites an individual 915 to be registered and individual 915 may for example be a litigant, etc. Individual 915 sits in front of an iris camera 917. On top of iris camera 917 is mounted a digital camera 919 on a swivel base. Digital camera 919 and iris camera 917 are connected to computer 905 which is in turn connected to a central database computer of the system through a link 921. Individual 915 is instructed by registrar 801 to sit an appropriate distance from and to look at digital camera 919. Registrar 801 can see the image of individual 915 on monitor 923 linked to computer 905. Registrar 801 captures a digital image of individual 915 by entering a command onto keyboard 903 or alternatively by using a mouse 927 linked to computer 905. The digital image is retained in computer memory in a file.

As one example of ensuring the correct distance and position for individual 915, registrar 801 instructs individual 915 to place his or her chin onto a chin rest

929 mounted in front of iris camera 917. Iris camera 917 is mounted on a swivel base 931 similar to the standard swivel base of optometry instruments such as slit lamps. Registrar 801 instructs individual 915 to hold still. Registrar 801 uses a joystick 933 of swivel base 931 to move iris camera 917 in the proper position to capture an in-focus image of the eye of individual 915 such as a standard in registration process for the system for example right eye. Registrar 801, upon seeing a sharply focused image of the right eye of individual 915 on monitor 923, inputs a command via mouse 927 to capture the image. The computer software algorithm analyses of the image of the iris of the right eye of individual 915 thus captured, prepares an iris code. A computer search is performed of the database of iris codes. This search determines if the right eye iris code of individual 915 matches any previously registered iris code. Where a match is found among the database, optionally, an image of the person with the matching previously registered iris code is displayed so that registrar 801 can determine if individual 915 is the previously registered person. Where no match is found, registrar 801 enters the digital image of individual 915 into the database and links the digital image of individual 915 to the data file of the iris code of individual 915. Similarly, registrar 801 also enters demographic data concerning individual 915 into the data file of individual 915 such as name, address, social security

number, presiding judge, attorney representing individual 915 and the like.

Where the judge has previously been registered by iris code (or any other appropriate biometric data), the entering of the name of the judge by registrar 801 into the file of individual 915 links the judges biometric to the biometric linked file of individual 915. Similarly, the entering of the judges name by registrar 801 in the data file of individual 915 optionally links the file of individual 915 to the audit trail of the judge. Any attorney representing individual 915 is similarly linked to the data file of individual 915 and to the judges file upon the attorneys name being entered by registrar 801. Optionally, individual 915, upon retaining an attorney, can consent to the attorneys access to the file of individual 915 by biometric consent. A bar code printer 935 linked to computer 905, in response to registrar 801 entering the biometrics of individual 915 into the database of the judge, prints a two dimensional bar code sticker 941 that registrar 801 places on a file 943, which is a hard copy file of the data of individual 915 in the court. When at some later time the judge scans sticker 941, computer 905 retrieves the file of individual 915 provided, optionally, that the judge is linked in the database as authorized to view the data file of individual 915. Bar code printer 935 can be any of several types as mentioned herein and the bar code can encode other information such as judge assigned

case, surrogate names of the registering individual, date, time, category of case, attorney representing individual 915, biometric data of registrar 801, and the like.

One embodiment of the invention concerns a litigant or human subject that requires a drug test per court order. To provide a complete understanding of how the present invention is integrated in a typical court system, the drug testing procedure is described in detail below. Some of the various forms required and used by the court (generally on computer monitor 923 of FIG. 12) are illustrated, for purposes of example only, in FIGS. 13 - 23. The system is made up of four functions, which are generally accessed by means of a main menu, illustrated specifically in FIG. 13. Court enrollment (used to register litigants with the system) and lab enrollment/recognition (used to register litigants with the system as well as confirm the identity of litigants sent from the courts) are very similar. Enter results is used by the lab technician to enter the specimen test results. Finally, view results is used by authorized persons to view the results of litigant tests. Each of the four functions will be discussed in the following sections.

The laboratory specimen and equipment required to carry out the drug testing consists of standard laboratory supplies and equipment that has been modified to accommodate the invention. To receive a drug test,

the litigant is first identified by driver's license or other standard means typically while in the court at the time of the judges order for the drug testing. The litigant may initially register at the courtroom at a desk type counter, as illustrated in FIG. 12 above, by providing a biometric reading via a biometric scanner. The biometric scanner is linked to a computer and preferably a bar code printer and scanner as described above. The biometric scanner or scanners may comprise one of a variety of conventional systems such as a fingerprint scanner available from the Ultra-Scan Corporation of Amherst, New York or an iris scanner available from IriScan corporation of Marlton, New Jersey. The bar code scanner and printer can be one of a variety available on the market such as from Nippon Denso of Japan or Symbol Technologies of Holtsville, New York

In this instance, when a litigant arrives at the court room registration desk, the court technician may instruct the litigant, for instance, to place his or her forefinger onto the biometric scanner during the registration process. The scanner takes or collects a biometric scan of the patients fingerprint which is digitized and sent to a computer which is linked to a computerized data system. This permits the court technician to link the fingerprint biometric scan to the court order for drug testing of the litigant with the computer. Optionally the litigant is also photographed

by a digital camera linked to the computer providing a recognizable photo of the litigant's face. The litigant may be provided with a demographic card bearing the litigants fingerprint biometric scan or smart card data or data preferably in the form of a two-dimensional bar code and the digital photo image.

Referring additionally to FIG. 14, a court enrollment menu is illustrated. To start the enrollment procedure for the enrollment of a new litigant, the enrollment button is pushed. The clerk focuses the image of the litigants eye on the screen and then presses the OK button. If the quality of the image is not high enough the system will reject it and the eye must be rescanned. If the image is accepted then the enrollment process continues and the clerk enters the litigants information in the spaces provided (see FIG. 15). In the SSN field only numbers are entered, the program enters the hyphens automatically. In the eye field right or left is entered, depending upon which eye was used for enrollment. When all of the information is entered the continue button is pressed to photograph the litigant. A get image button (not shown) is pressed to start the photograph process. If necessary, an adjustment to the brightness is made. To adjust the brightness and contrast the clerk removes a check from an automatic brightness box (not shown) and then uses sliders to correct the brightness and contrast levels. A take a picture button is then pressed to take the

photograph. To transfer the photograph to storage a transfer button is pressed or to retake the photo a try again button is pressed. After the transfer button is pressed and the photograph is in the file, the photo process is exited by pressing the close button. If the picture was taken correctly, it will appear on the screen, as illustrated in FIG. 16. If there is no picture on the screen, the get image button is pressed again and the above steps are repeated, otherwise the continue button is pressed.

The final screen, illustrated in FIG. 16, of the enrollment process shows all of the information about the litigant that was enrolled, including the photograph. From this screen the litigants photograph can be permanently saved without change or optionally updated if authorized. To update the photograph, press the update picture 1 button to start the photo process. When the update picture 1 button is pressed, picture 1 is replaced by the new photograph. If the update picture 2 button is pressed, then the image will be placed in the picture 2 box. When the final enrollment screen is displayed, one litigant bar code will be printed. Only one litigant bar code can be printed per scan of the eye. If another litigant bar code label is needed, the litigants eye must be scanned again. If an eye of a litigant that is already registered with the system is scanned, the enrollment procedure will skip to the final enrollment screen and display the information

previously entered. This information can then be corrected if necessary.

The procedure to enroll a new litigant to the system is the same as at the court, the only difference being the specimen bar codes that will be printed. To enroll an individual, the enrollment button in the lab enrollment/recognition menu (see FIG. 17) is pressed and the steps detailed above for the court enrollment function are followed. To recognize a litigant sent from the court, the recognition button (FIG. 17) is pressed. Upon completion of a successful enrollment or recognition, options will be presented to update the pictures or to print specimen bar codes. As in the court enrollment, only one litigant bar code is printed with every scan of the eye. However, the specimen bar codes can be generated as needed until the screen is closed. Once the screen is closed, the litigants eye must be scanned again to print additional bar codes (litigant or specimen). To print a specimen bar code, enter a control number into the space provided, then press the specimen button. The bar code is then affixed to the specimen.

To enter results of a test to the system, the "enter results" button is pressed. When prompted (see FIG. 19), the specimen bar code is scanned. The results are entered into the spaces provided (see FIG. 20) and the exit button is pressed after completion. To modify any results entered into the system, the enter results

button from the main menu (FIG. 13) is pressed and the specimen bar code is scanned again.

To view a litigants test results, the "view results" button of the main menu (FIG. 9) is pressed. When prompted (see FIG. 21), the litigant bar code is scanned. A view results screen will then appear, as illustrated in FIG. 22. No information can be modified from this screen. Anyone logging on to the system starts the software by double clicking on an appropriate icon on the desk top monitor (e.g. monitor 923 of FIG. 12). The log on dialog box illustrated in FIG. 23 appears on the monitor. The operator enters the users name followed by his or her password. The password is case sensitive and must be typed exactly as assigned.

The instant invention is envisioned to be useful in connection with data files used in the professional activities of other professionals such as physician, pharmacist, chiropractor, surrogate of licensed professional, patient, dentist, dental hygienist, medical technologist, nurse, surgeon, emergency medical technician, medical assistant, lawyer, broker, physician assistant, optometrist, optometry technician, healthcare workers, transportation workers and the like. In this respect these professionals are envisioned to use the system for such activities as continuing education documents, re-credentialing, certification, secure communications, work records, accident history, audit of data transfer and the like.

The system herein disclosed is envisioned for home use where for example a lawyer is retained over the telephone or alternatively during home to attorney office video conference. In this circumstance, the client at home transmits authorization for the attorney to access client files in the database of the system computer. The data of a client biometric can be matched on a one-to-one basis in the home computer against a code sent to the computer by the central computer in response to the client providing a client name over the phone. The match is confirmed prior to transmission of documents or authorization. Alternatively, the biometric can be sent as data to the central computer, preferably over cable modem lines or other high data transfer rate lines. This latter type of one-to-many match is preferable because the client biometric code is not sent out from the central computer to other sites thus reducing the possibility of hacking the data during transmission or later from off-site.

Other uses envisioned for the instant invention include security of documents such as involved in corporate security and government security. The biometric codes of users is envisioned linked to level of authorization to information such as "eyes only" access.

Still other embodiments are possible within the scope of the invention herein disclosed and those other embodiments are intended to be included in the invention

herein disclosed. For example the cellular telephone with built in biometric iris scanner is envisioned to be useful for verification of identity of the user of the telephone in relation to access and authority to access and copy files of the system. In another example the instant invention is envisioned to be used where the attorney is providing his biometric data to a computer containing a database of encoded biometric data used to authorize various legal services and activities such as consent to a settlement or agreement to a contract. Similarly, the instant invention of the website-based use of computer matching of encoded biometric data is envisioned to be useful in a variety of legal uses including the Internet linked website receipt of identity verification of the individual attorney surrogate. Also, one skilled in the art will realize that biometric measurements or data can be encoded on a storage medium by the computers to which the various sampling devices are coupled, by the sampling devices themselves, which read the biometric measurements or data or any combination thereof. Furthermore, the encoded biometric data may be sent to a remote site for storage either electronically or by hard copy. For example, as detailed in the previous description, the encoded biometric data may be in the form of a two-dimensional bar code.

Thus, the above described problems and others are at least partially solved and the above described

purposes and others are realized in improved methods, systems and apparatus for preparing, linking, filing, accessing, sorting, retrieving, transmitting and auditing of documents and in particular in linking said documents to the identity of individuals associated with the document. The association for which the link is established can be one of several relationships such as a principal for whom the document pertains, an individual for whom access is granted, an individual authorizing action disclosed in document, etc. As a preferred embodiment, improved methods, systems and apparatus are disclosed for linking of legal documents such as court mandated drug testing reports to the identity of the following individuals: the subject of the testing, the judge who orders the test, the attorney for the tested subject, the bailiff transporting litigant, the bailiff registering the litigant and the clerk authorized to access and review the test results. It is understood that both legal and non-legal documents are envisioned to be included within the scope of the instant invention.

It is understood that the invention herein disclosed as preferred embodiments is for illustrative purposes. Various changes and modifications to the embodiments herein chosen for purposes of illustration will readily occur to those skilled in the art. For example the auditing of activities by biometric code is optionally envisioned to be by bar code scan wherein the

iris code of an individual is encoded into the bar code. The authorization to view the audit report is preferably by iris scanner scan of iris of a person seeking authority. The activities thus available to be searched and reported include which documents were sent or received by a particular individual, when such documents were transferred, the location to which the document was sent and the person receiving data as well as the method used to transfer the data such as fax machine number, e-mail address, copier node and the like. To the extent such modifications and variations do not depart from the spirit of the invention, they are intended to be included within the scope thereof which is assessed only by a fair interpretation of the following claims.

Having fully described the invention in such clear and concise terms as to enable those skilled in the art to understand and practice the same, the invention claimed is:

CLAIMS

1. A method for the authorization of documents comprising the steps of:

preparing a record for future reference by authorized personnel including providing a document including data pertaining to an individual, collecting biometric data from the individual and forming a code including the biometric data, attaching the code to the document, and storing the document and attached bar ; and

authenticating the document and attached code upon removal from storage by collecting current biometric data from a person allegedly the individual, comparing the current biometric data to the biometric data included in the code, and

confirming by a positive comparison that the person and the individual are identical and that the document pertains to the person and the individual, and authorizing the removal of the document from storage.

2. A method for the authorization of documents as set forth in claim 1 wherein the steps of collecting biometric data from the individual and collecting current biometric data from the person include one of scanning an iris of the individual and the person, taking a finger print of the individual and the person, acquiring a signature of the individual and the person,

and acquiring a voice print of the individual and the person.

3. A method for the authorization of documents as set forth in claim 1 wherein the steps of preparing the record and authenticating the document each further include a step of taking a digital photograph of the individual and taking a digital photograph of the person, respectively.

4. A method for the authorization of documents as set forth in claim 1 wherein the step of forming the code including the biometric data includes forming one of a two-dimensional bar code, a cross-hatched bar code, a bar code with a non-copy background, and bar codes that are readable by one of optical or magnetic means.

5. A method for the authorization of documents as set forth in claim 1 wherein the step of authenticating the document and attached code upon removal from storage includes removal from storage by means of one of the following: a computer system, an Internet system, a facsimile system, and a copier.

6. A method for the authorization of documents comprising the steps of:

preparing a record for future reference by authorized personnel including providing a document,

collecting biometric data from an individual requesting authority to become an authorized person to access the document, forming a code including the biometric data from the individual, attaching the code to the document, and storing the document and attached code;

authorizing access to the document by collecting current biometric data from a person requesting access to the document, comparing the current biometric data to the code attached to the document, and confirming by a positive comparison that the person requesting access and the individual are identical and that the person has authority to access the document.

7. A method for the authorization of documents as set forth in claim 6 wherein the steps of collecting biometric data from the individual and collecting current biometric data from the person include one of scanning an iris of the individual and the person, taking a finger print of the individual and the person, acquiring a palm print hand geometry, signature of the individual and the person, and acquiring a voice print of the individual and the person.

8. A method for the authorization of documents as set forth in claim 6 wherein the steps of preparing the record and authenticating the document each further include a step of taking a digital photograph of the

individual and taking a digital photograph of the person, respectively.

9. A method for the authorization of documents as set forth in claim 6 wherein the step of forming the code including the biometric data includes forming one of a two-dimensional bar code, a cross-hatched bar code, a bar code with a non-copy background, and bar codes that are readable by one of optical or magnetic means.

10. A method for the authorization of documents as set forth in claim 6 wherein the step of authenticating the document and attached code upon removal from storage includes removal from storage by means of one of the following: a computer system, an Internet system, a facsimile system, and a copier.

11. A method for the authorization of documents as set forth in claim 6 wherein the steps of collecting biometric data from the individual requesting authority and forming a code is repeated for each individual requesting authority and the code containing biometric data for each individual requesting authority is attached to the document.

12. A method for the authorization of documents comprising the steps of:

preparing a record for future reference by authorized personnel including providing a document including data pertaining to an individual, collecting biometric data from the individual and forming a bar code including the biometric data, attaching the bar code to the document, and storing the document and attached bar code;

authenticating the document and attached bar code by collecting current biometric data from a person allegedly the individual, comparing the current biometric data to the biometric data included in the bar code, and confirming that the person and the individual are identical and that the document pertains to the person and the individual;

preparing the document for future access by authorized personnel including collecting biometric data from an individual requesting authority to become an authorized person to access the document, forming a bar code including the biometric data from the individual requesting authority, attaching the bar code to the document, and storing the document and attached bar code; and

authorizing access to the document by collecting current biometric data from a person requesting access to the document, comparing the current biometric data to the bar code attached to the document, and confirming that the person requesting access and the individual are

identical and that the person has authority to access the document.

13. A method for the authorization of documents as set forth in claim 12 wherein the steps of collecting biometric data from the individual, collecting current biometric data from the person allegedly the individual, collecting biometric data from an individual requesting authority, and collecting current biometric data from a person requesting access include one of scanning an iris of the individual and the person, taking a finger print of the individual and the person, acquiring a signature of the individual and the person, and acquiring a voice print of the individual and the person.

14. A method for the authorization of documents as set forth in claim 12 wherein the steps of preparing the record and authenticating the document each further include a step of taking a digital photograph of the individual and taking a digital photograph of the person, respectively.

15. A method for the authorization of documents as set forth in claim 14 wherein the step of taking a digital photograph of the individual includes dividing the digital photograph into first and second partial images, storing the first partial image linked to a first portion of the biometric data from the individual

and the second partial image linked to a second portion of the biometric data from the individual, and verifying the individual by comparing first and second portions of the current biometric data to the stored first and second portions of the biometric data and forming a composite image of the linked first and second partial images.

16. A method for the authorization of documents as set forth in claim 12 wherein the steps of preparing the document for future access by authorized personnel and authorizing access to the document each further include a step of taking a digital photograph of the individual and taking a digital photograph of the person, respectively.

17. A method for the authorization of documents as set forth in claim 12 wherein the steps of forming the bar code including the biometric data each include forming one of a two-dimensional bar code, a cross-hatched bar code, a bar code with a non-copy background, and bar codes that are readable by one of optical or magnetic means.

18. A method for the authorization of documents as set forth in claim 12 wherein the step of authorizing access to the document includes access by means of one

of the following: a computer system, an Internet system, a facsimile system, and a copier.

19. A method for the authorization of documents as set forth in claim 12 wherein the steps of collecting biometric data from the individual requesting authority and forming a bar code is repeated for each individual requesting authority and the bar code containing biometric data for each individual requesting authority is attached to the document.

20. A method of verifying the operation of biometric apparatus comprising the following steps performed in any operative order:

taking a digital photograph and electronically dividing the digital photograph into first and second portions;

collecting and storing first biometric data from an individual;

linking the first portion of the digital photograph to the stored first biometric data and storing the linked first portion of the digital photograph;

collecting and storing second biometric data, different from the first biometric data, from the individual;

linking the second portion of the digital photograph to the stored second biometric data and

storing the linked second portion of the digital photograph;

collecting current first biometric data from the individual;

comparing the current first biometric data to the stored first biometric data and displaying the stored first portion of the digital photograph;

collecting current second biometric data from the individual; and

comparing the current second biometric data to the stored second biometric data and displaying the stored second portion of the digital photograph as a composite photograph in combination with the first portion of the digital photograph.

21. A method of verifying the operation of biometric apparatus as claimed in claim 20 wherein the first and second biometric data include right and left iris scans, respectively, and the first and second current biometric data include right and left iris scans, respectively.

22. A method of verifying the operation of biometric apparatus as claimed in claim 20 wherein the first and second portions of the digital photograph include alternate arcuate sections.

23. A method of verifying the operation of biometric apparatus as claimed in claim 20 wherein the first and second portions of the digital photograph include alternate horizontal scan lines.

24. Apparatus for authorization to access documents comprising:

a document, a bar code including biometric data from an authorized individual attached to the document;

apparatus for collecting current biometric data from a person requesting access to the document; and

comparing means, including a bar code reader, for comparing the current biometric data to the bar code attached to the document to confirm by a positive comparison that the person requesting access and the authorized individual are identical and that the person has authority to access the document.

25. Apparatus for authorization to access documents as set forth in claim 24 wherein the biometric data included in the bar code and the current biometric data collected by the apparatus include one of an iris scan of the individual and the person, a finger print of the individual and the person, a signature of the individual and the person, and a voice print of the individual and the person.

26. Apparatus for authorization to access documents as set forth in claim 24 wherein the document further includes a digital photograph of the individual and the comparing means includes a camera for taking a digital photograph of the person, respectively.

27. Apparatus for authorization to access documents as set forth in claim 24 wherein the bar code includes one of a two-dimensional bar code, a cross-hatched bar code, a bar code with a non-copy background, and bar codes that are readable by one of optical or magnetic means.

28. Apparatus for authorization to access documents as set forth in claim 24 wherein the apparatus for collecting current biometric data from a person requesting access to the document includes one of the following: a computer system, an Internet system, a facsimile system, and a copier.

29. Apparatus for authorization to access documents as set forth in claim 24 wherein a plurality of individuals are authorized access to the document and a bar code including biometric data from each authorized individual is attached to the document.

30. Apparatus for authorization of documents comprising:

a document including data pertaining to an individual and a bar code including biometric data from the individual attached to the document;

apparatus for collecting current biometric data from a person allegedly the individual; and

comparing means, including a bar code reader, for comparing the current biometric data to the biometric data included in the bar code, and confirming by a positive comparison that the person and the individual are identical and that the document pertains to the person and the individual.

31. A system for sorting documents wherein the biometric data of a person is identified as linked to the sorting document.

32. The system of claim 31 wherein the person is the subject of the data in the document.

33. The system of claim 31 wherein the sorting is authorized via biometric code of user.

34. The system of claim 33 wherein the user authorization is auditable.

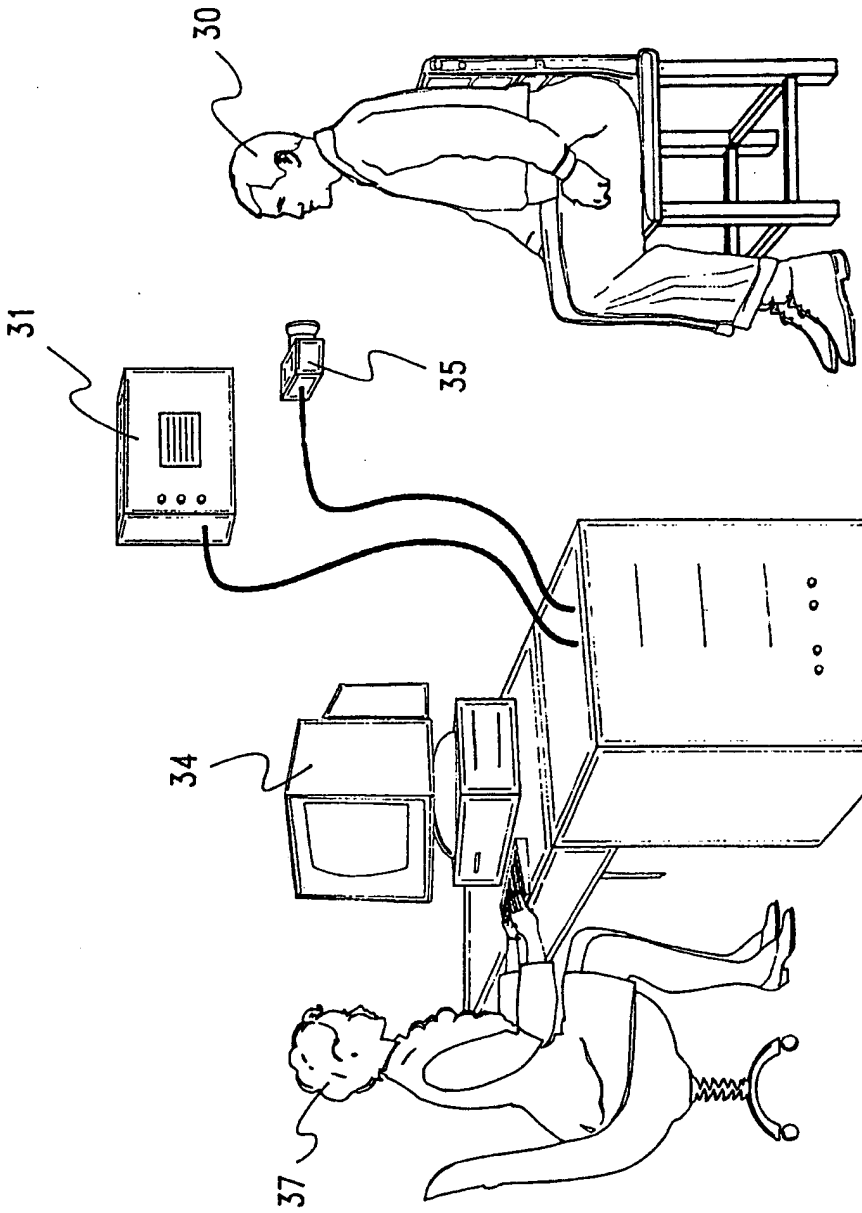



Fig. 1

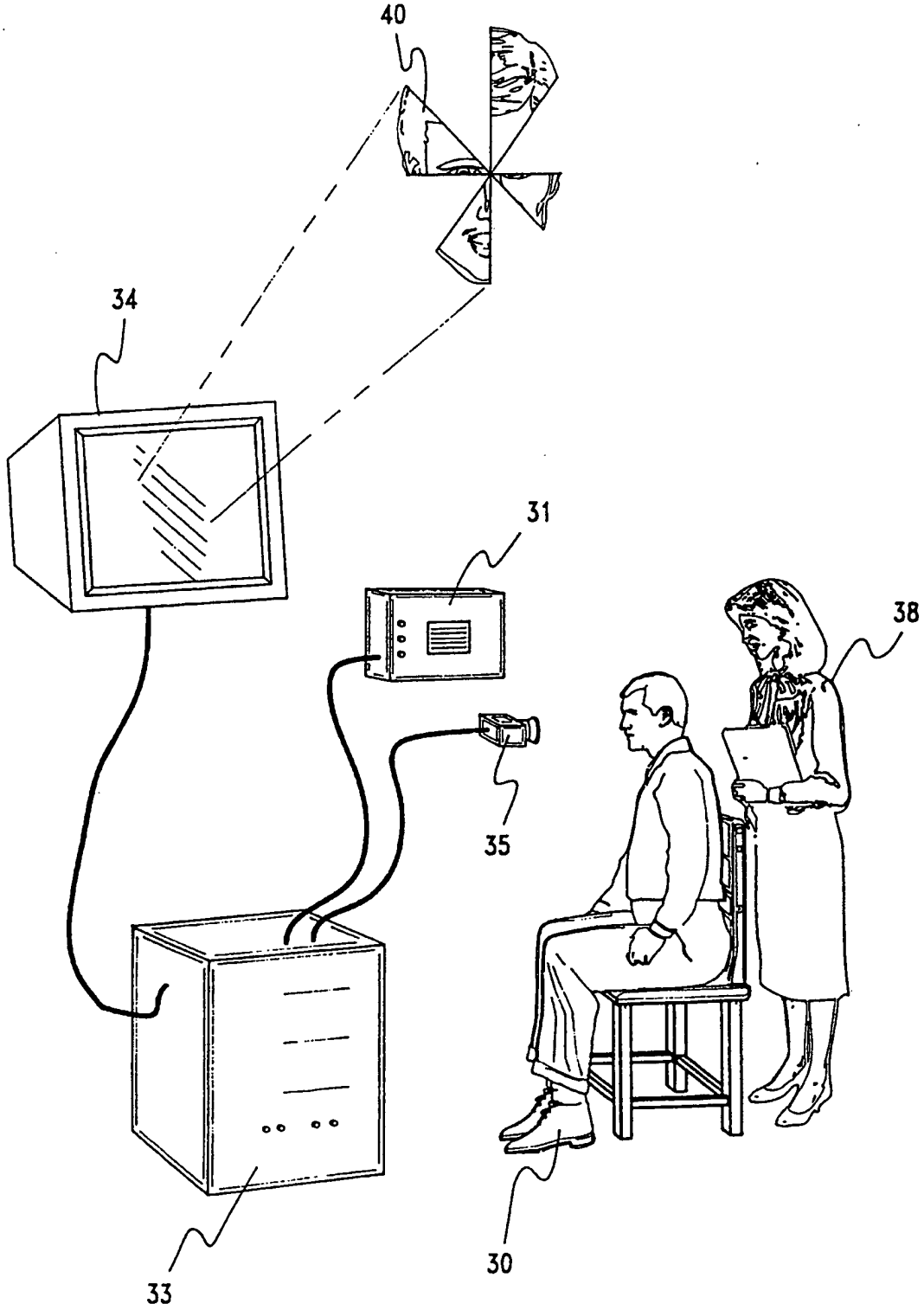



Fig. 2

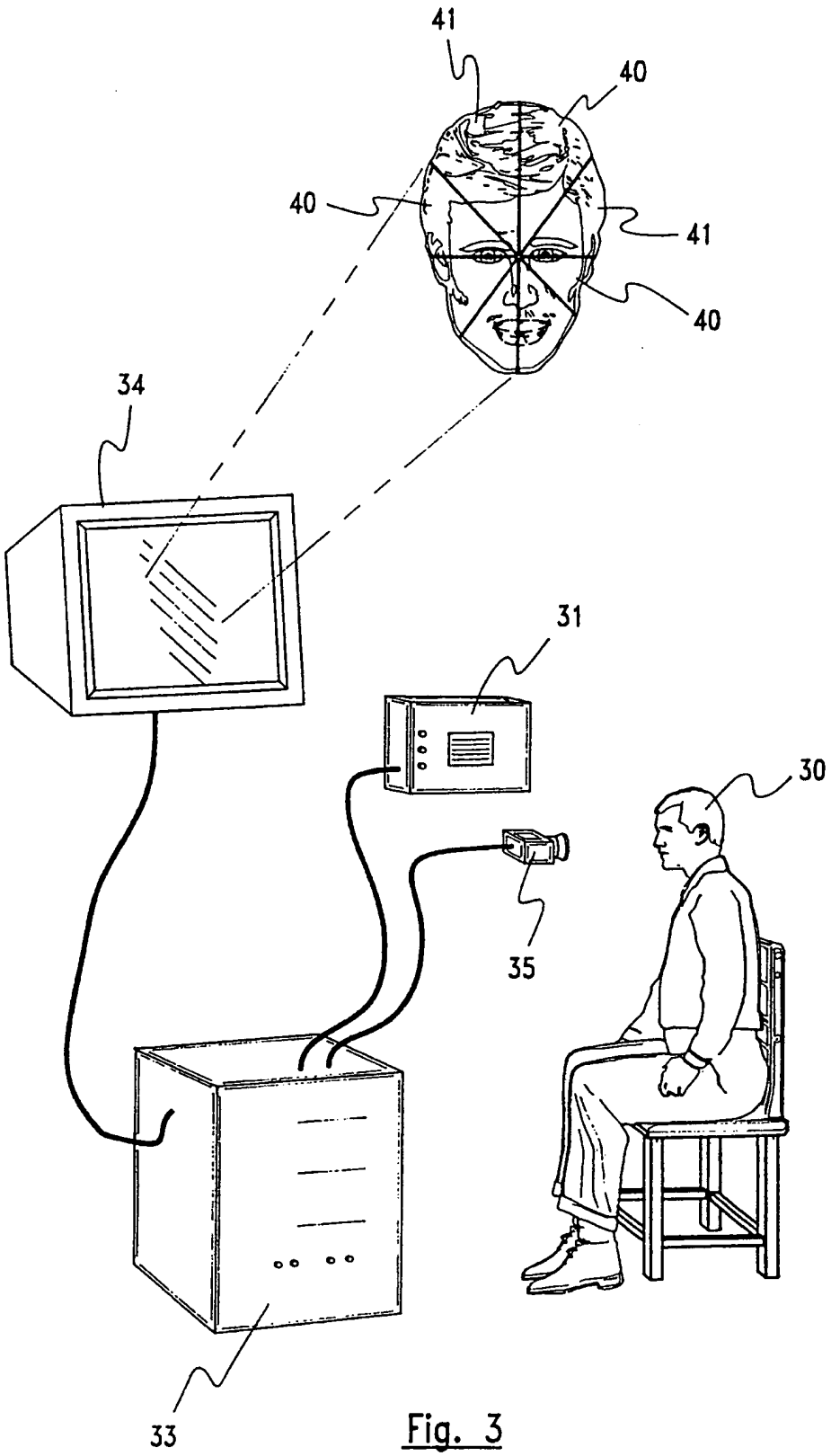



Fig. 3

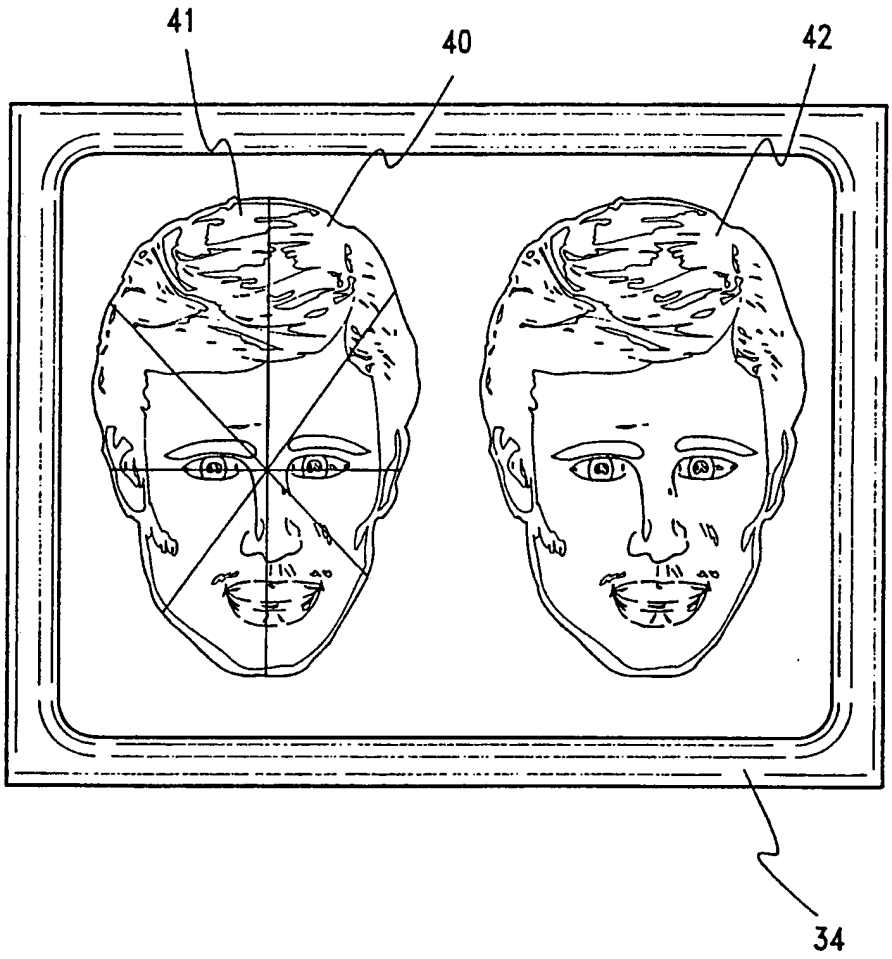



Fig. 4

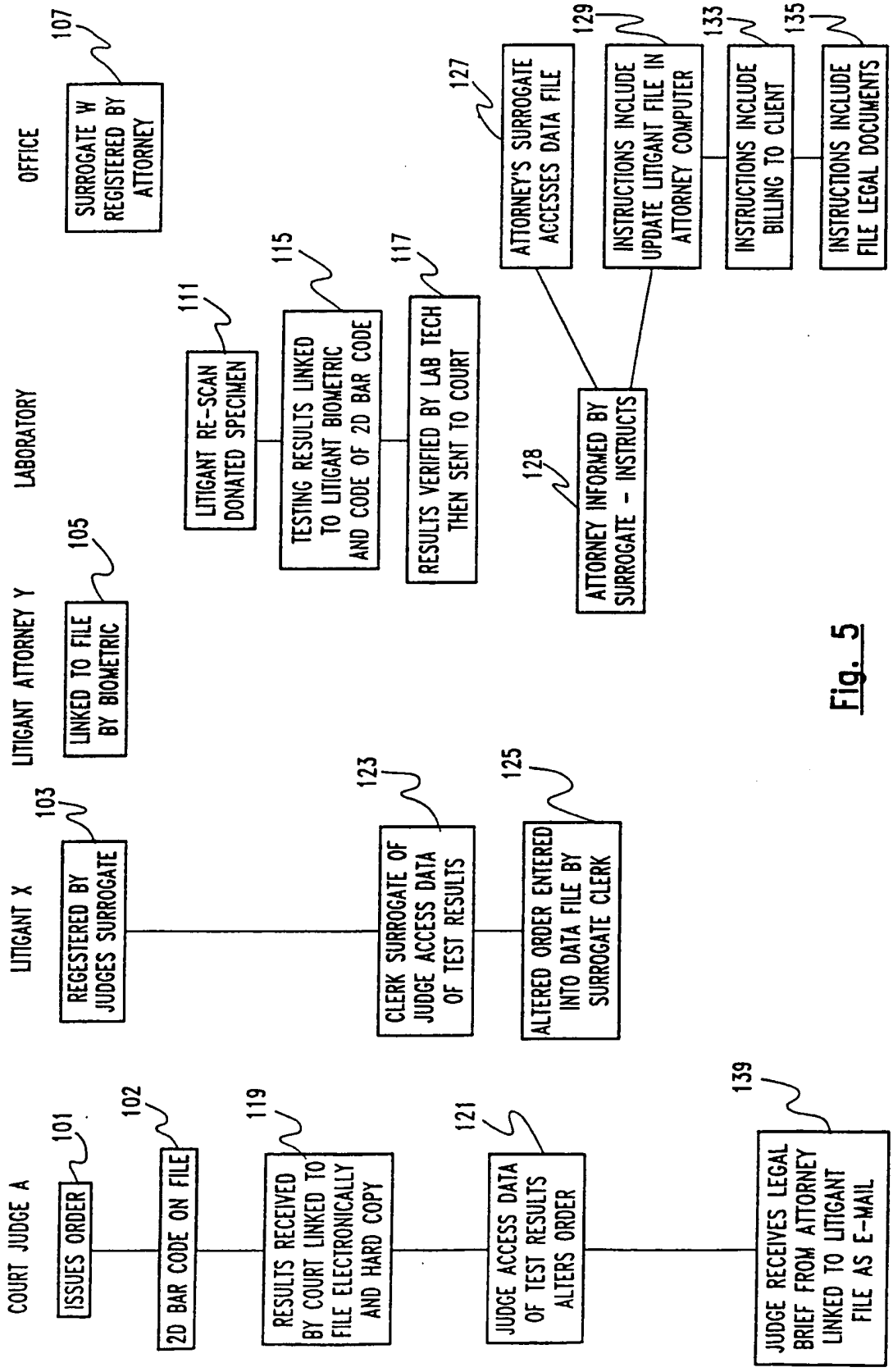

COURT JUDGE A
ISSUES ORDER
101
2D BAR CODE ON FILE
102
RESULTS RECEIVED BY COURT LINKED TO FILE ELECTRONICALLY AND HARD COPY
119
JUDGE ACCESS DATA OF TEST RESULTS ALTERS ORDER
121
JUDGE RECEIVES LEGAL BRIEF FROM ATTORNEY LINKED TO LITIGANT FILE AS E-MAIL
139
LITIGANT X
REGESTERED BY JUDGES SURROGATE
103
CLERK SURROGATE OF JUDGE ACCESS DATA OF TEST RESULTS
123
ALTERED ORDER ENTERED INTO DATA FILE BY SURROGATE CLERK
125
LITIGANT ATTORNEY Y
LINKED TO FILE BY BIOMETRIC
105
LABORATORY
LITIGANT RE-SCAN DONATED SPECIMEN
111
TESTING RESULTS LINKED TO LITIGANT BIOMETRIC AND CODE OF 2D BAR CODE
115
RESULTS VERIFIED BY LAB TECH THEN SENT TO COURT
117
ATTORNEY INFORMED BY SURROGATE - INSTRUCTS
128
OFFICE
SURROGATE W REGISTERED BY ATTORNEY
107
ATTORNEY'S SURROGATE ACCESSES DATA FILE
127
INSTRUCTIONS INCLUDE UPDATE LITIGANT FILE IN ATTORNEY COMPUTER
129
INSTRUCTIONS INCLUDE BILLING TO CLIENT
133
INSTRUCTIONS INCLUDE FILE LEGAL DOCUMENTS
135

Fig. 5

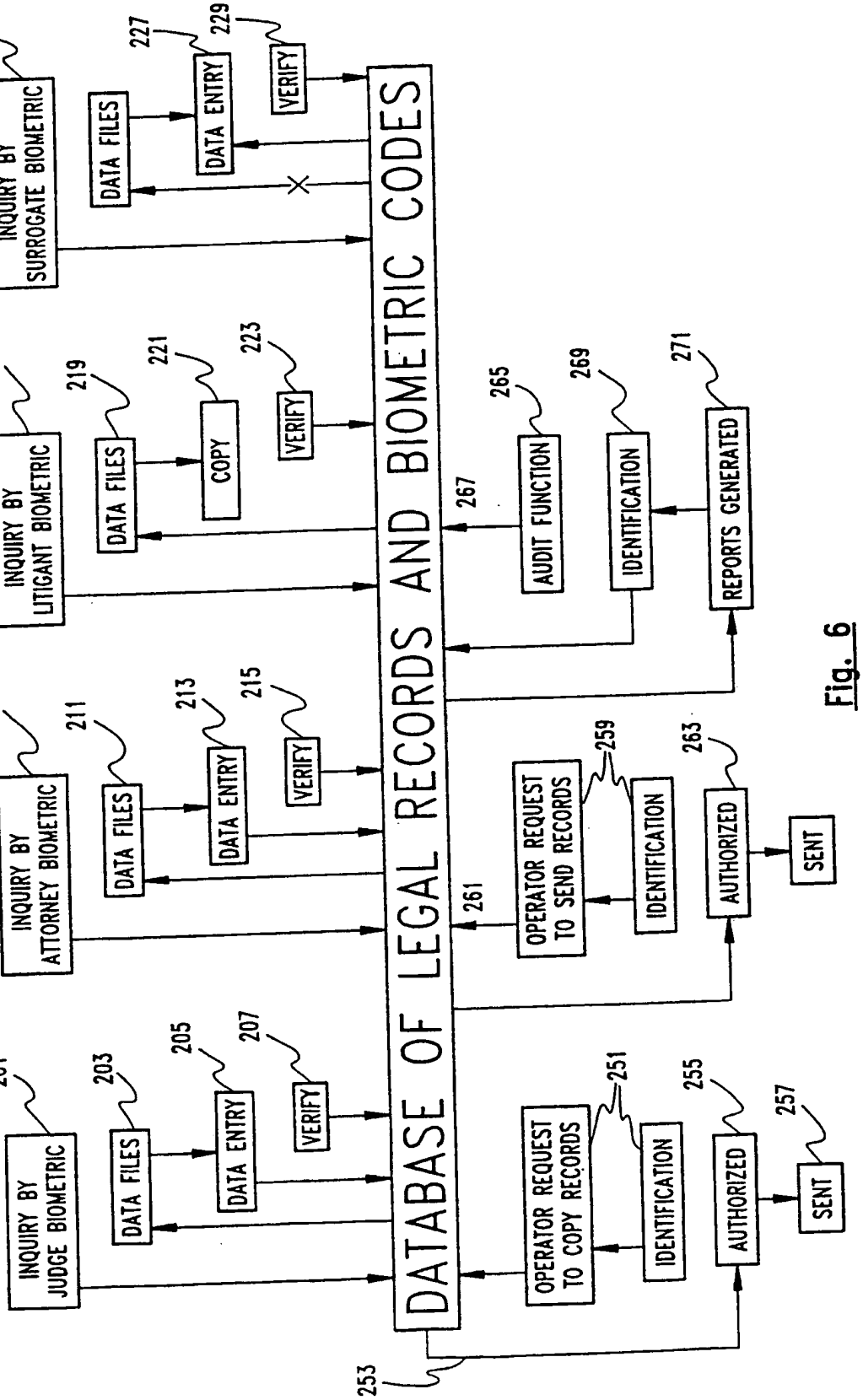

DATABASE OF LEGAL RECORDS AND BIOMETRIC CODES
INQUIRY BY JUDGE BIOMETRIC
201
DATA FILES
203
DATA ENTRY
205
VERIFY
207
INQUIRY BY ATTORNEY BIOMETRIC
209
DATA FILES
211
DATA ENTRY
213
VERIFY
215
INQUIRY BY LITIGANT BIOMETRIC
217
DATA FILES
219
COPY
221
VERIFY
223
INQUIRY BY SURROGATE BIOMETRIC
225
DATA FILES
227
DATA ENTRY
229
VERIFY
253
OPERATOR REQUEST TO COPY RECORDS
251
IDENTIFICATION
AUTHORIZED
255
SENT
257
OPERATOR REQUEST TO SEND RECORDS
259
IDENTIFICATION
AUTHORIZED
263
SENT
261
AUDIT FUNCTION
265
IDENTIFICATION
269
REPORTS GENERATED
271
267

Fig. 6

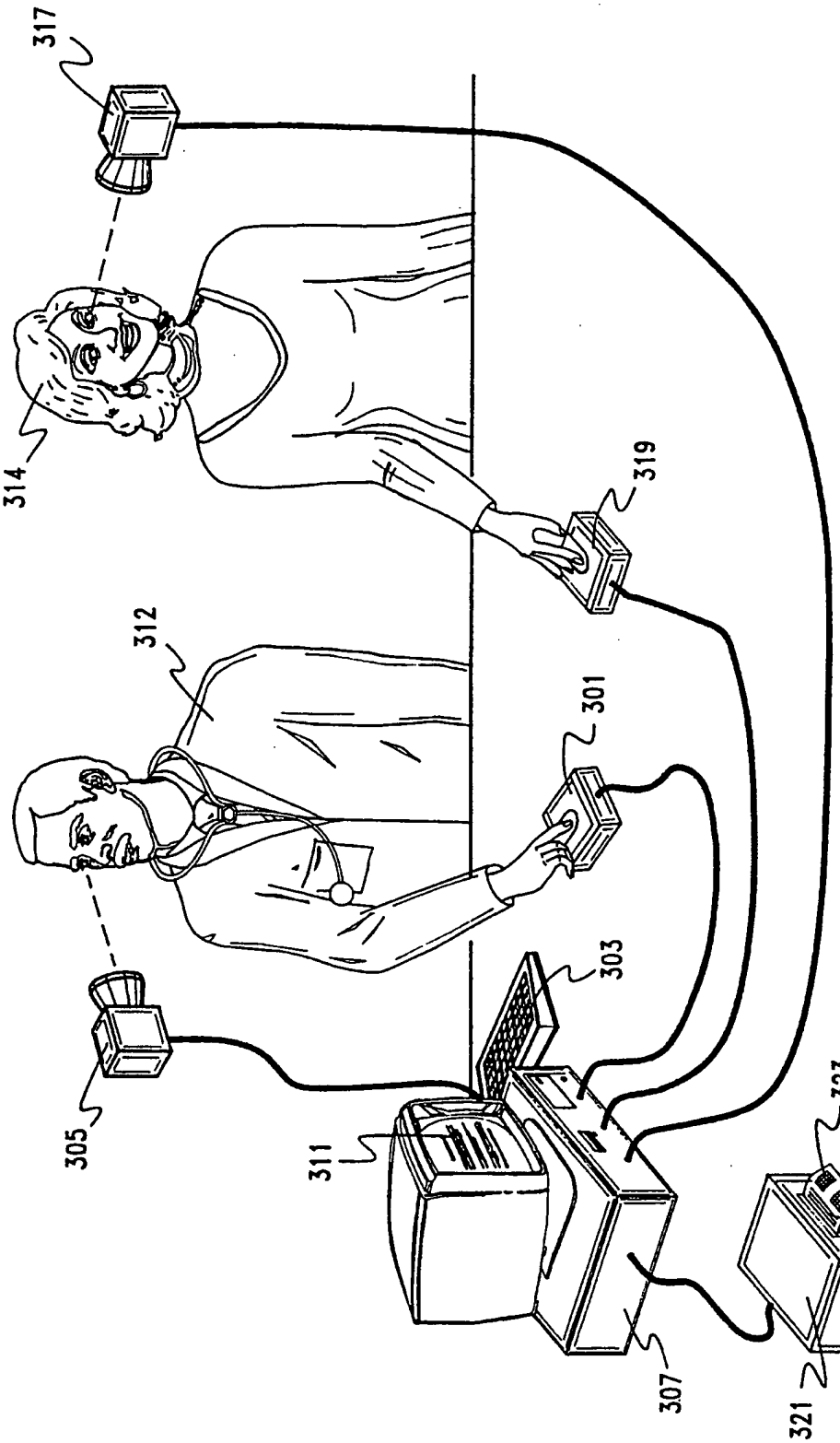



Fig 7

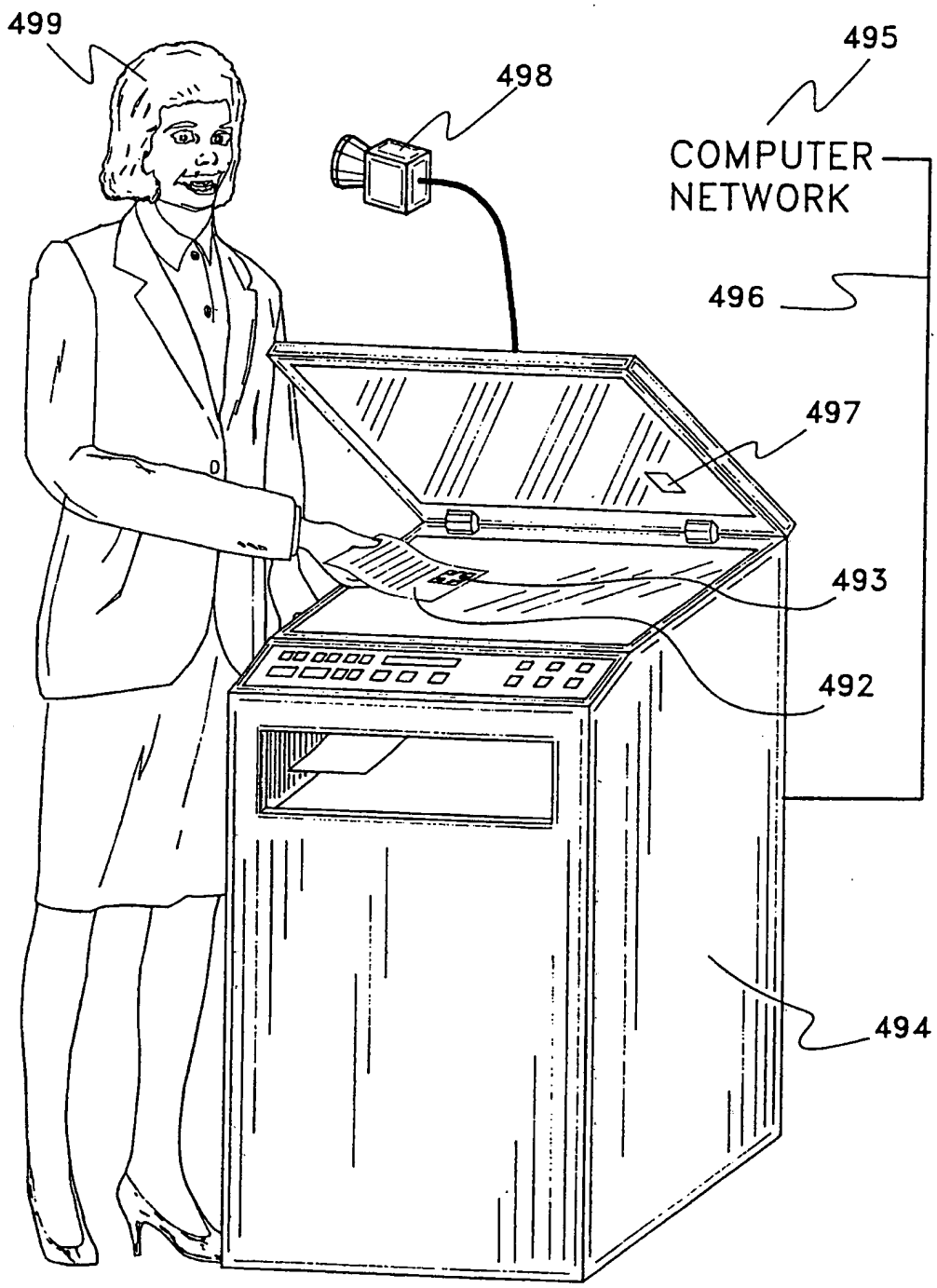



Fig. 8

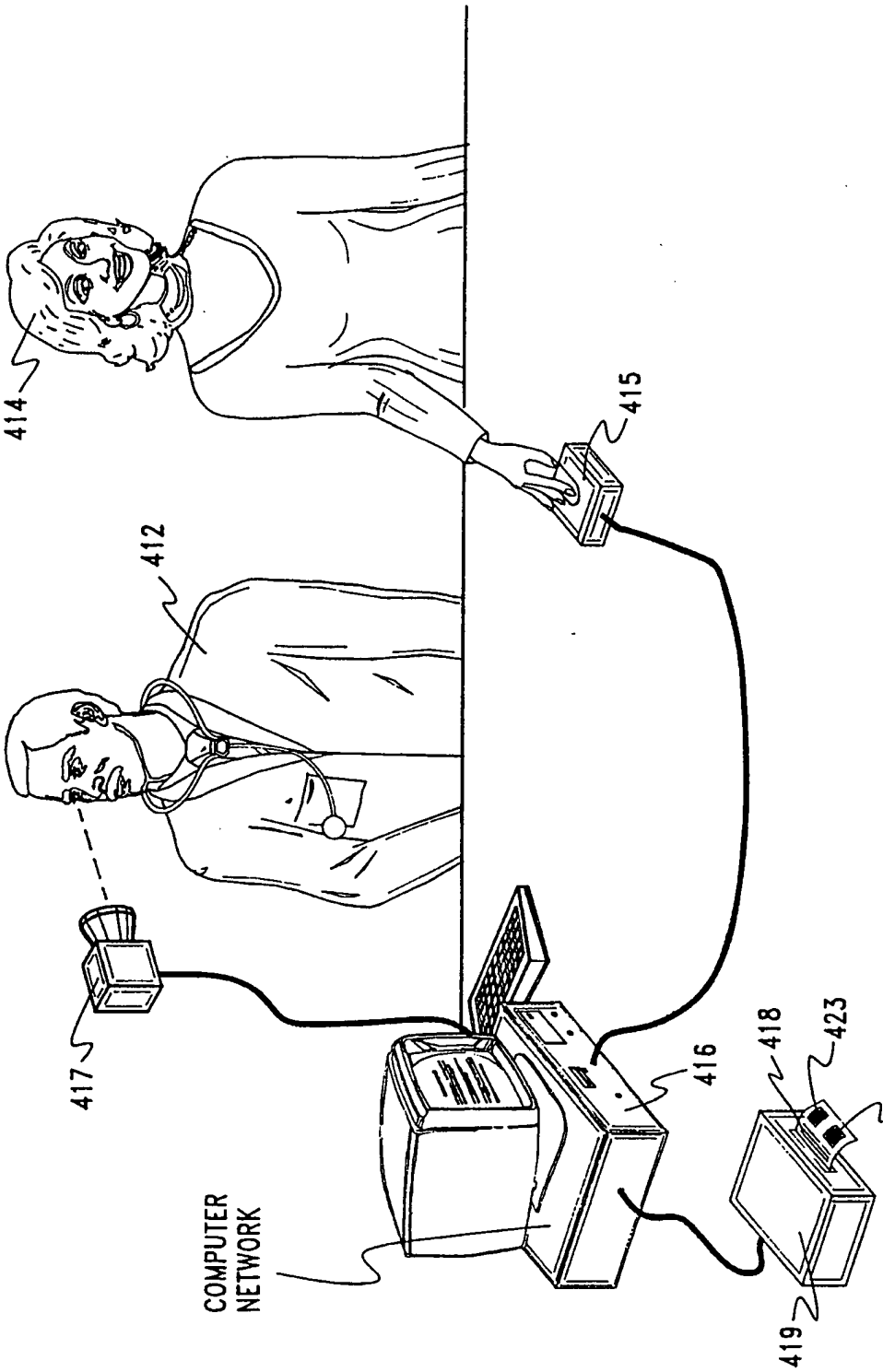



Fig 9

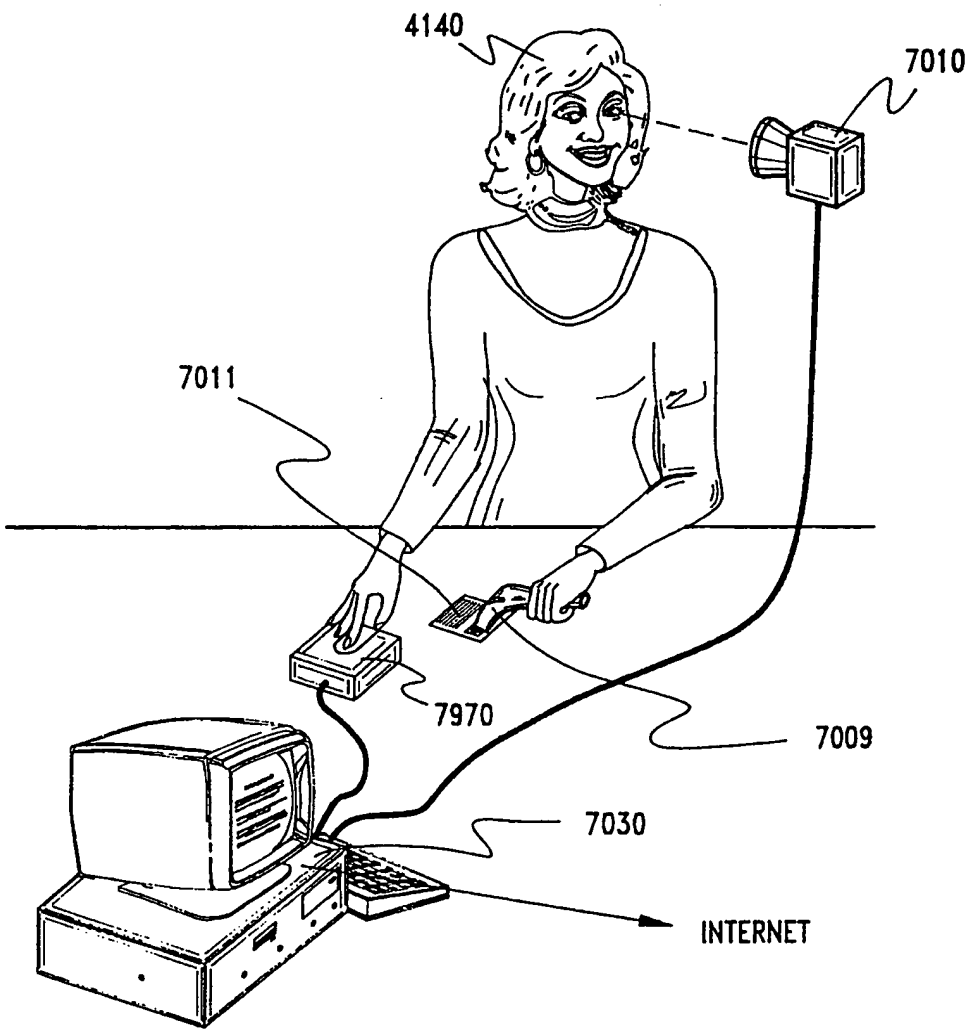



Fig 10

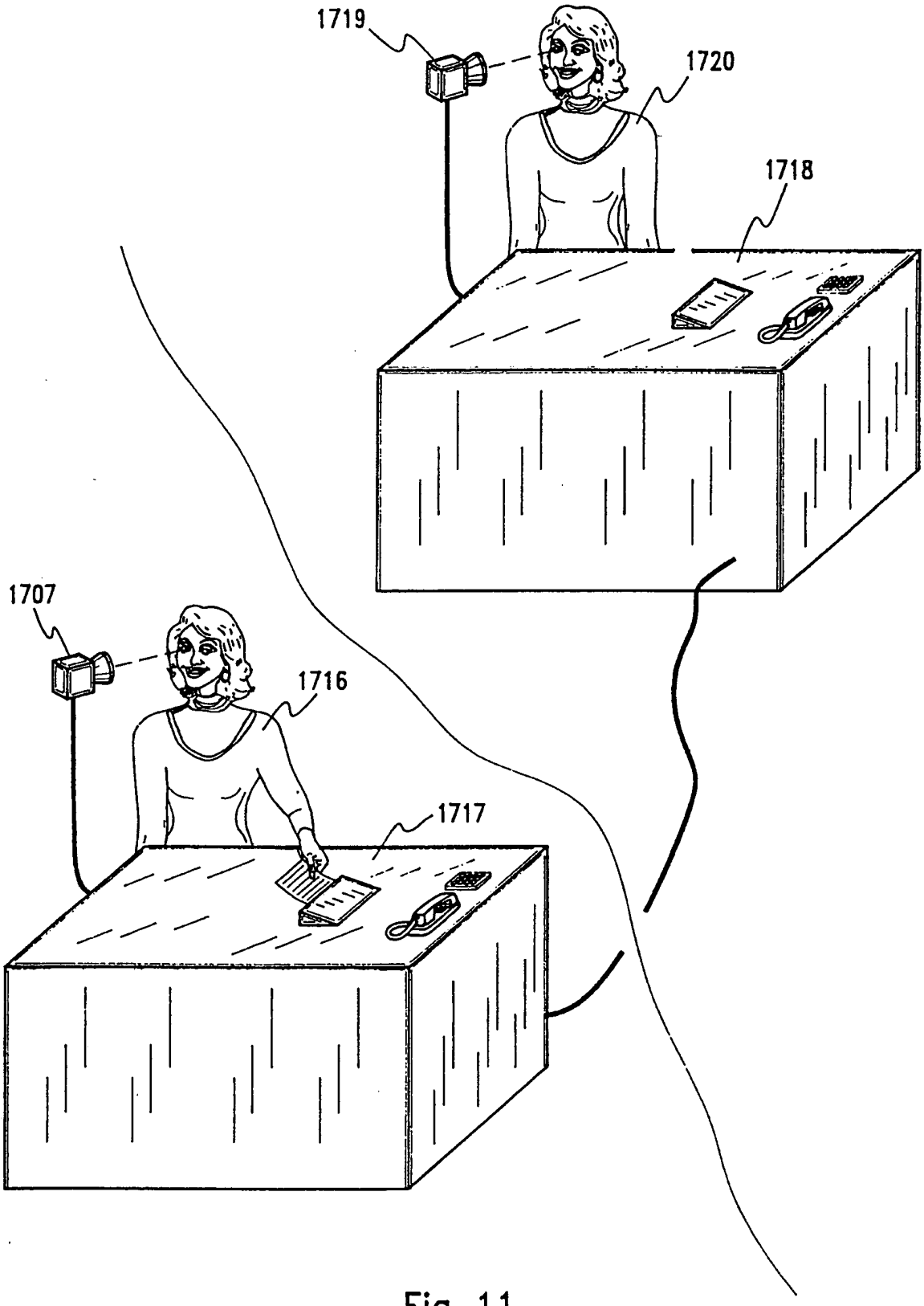



Fig 11

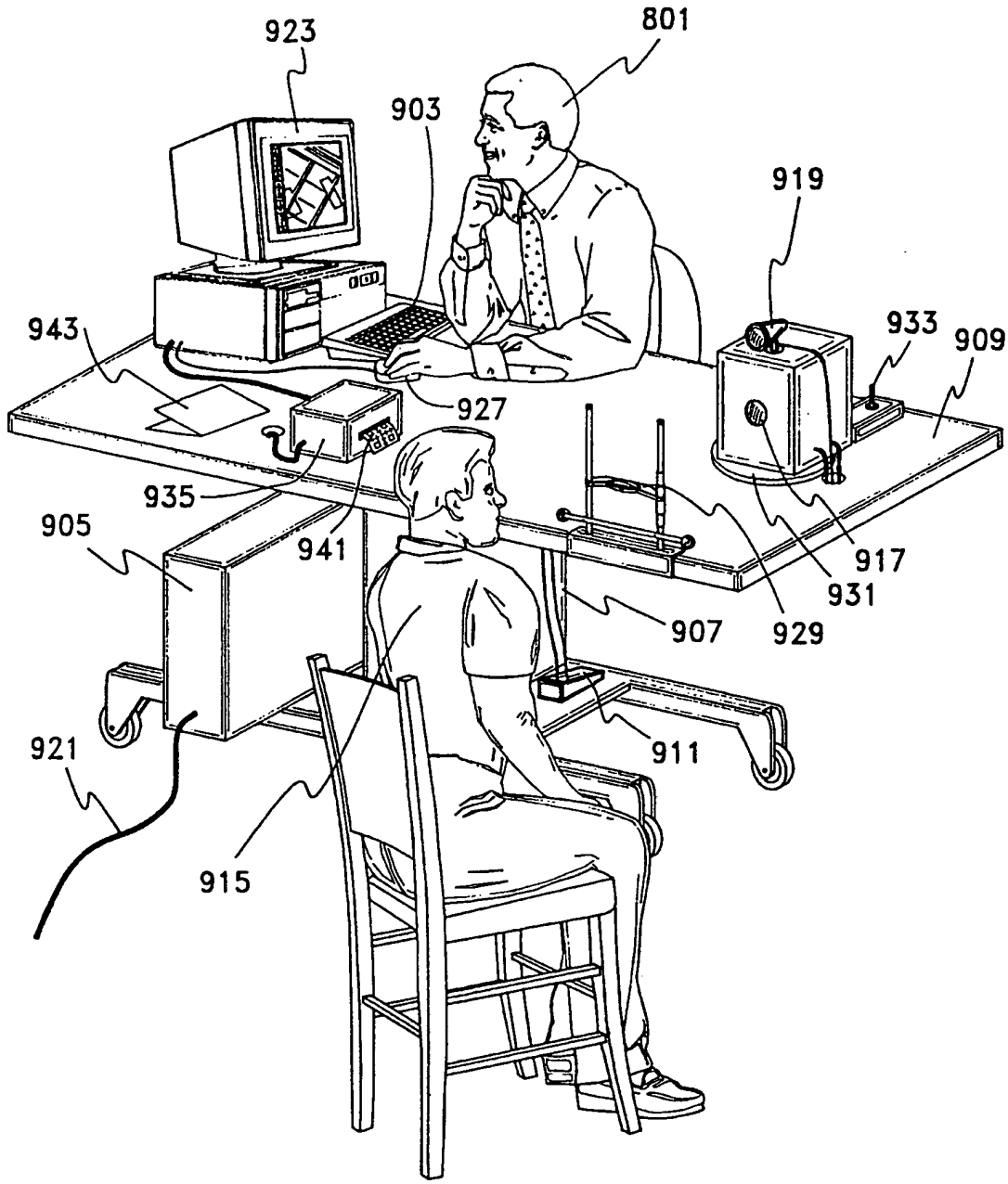

923
801
903
919
943
933
909
927
935
905
941
917
931
907
929
921
911
915

Fig 12

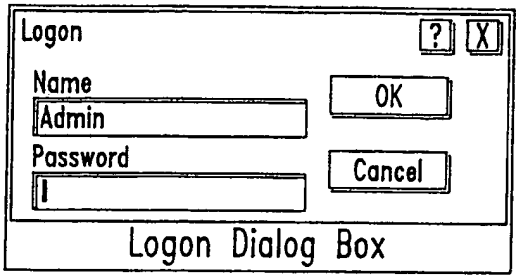



Fig. 23

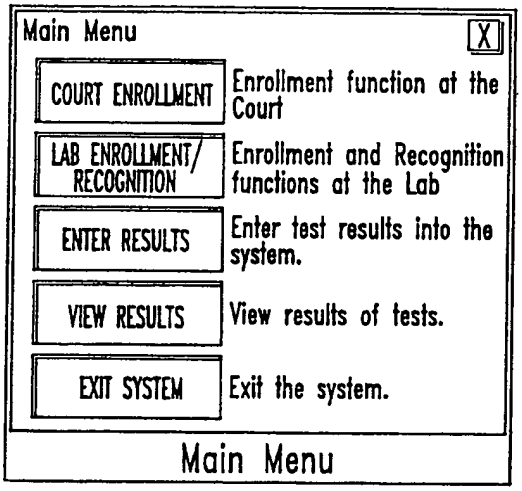



Fig. 13

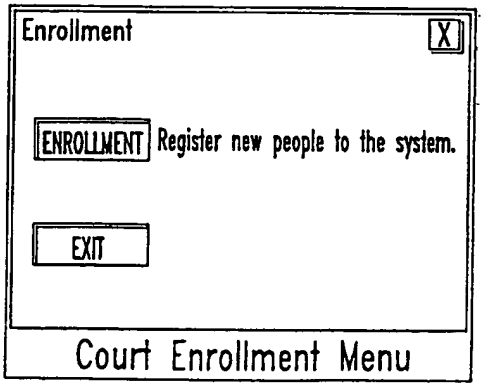



Fig. 14

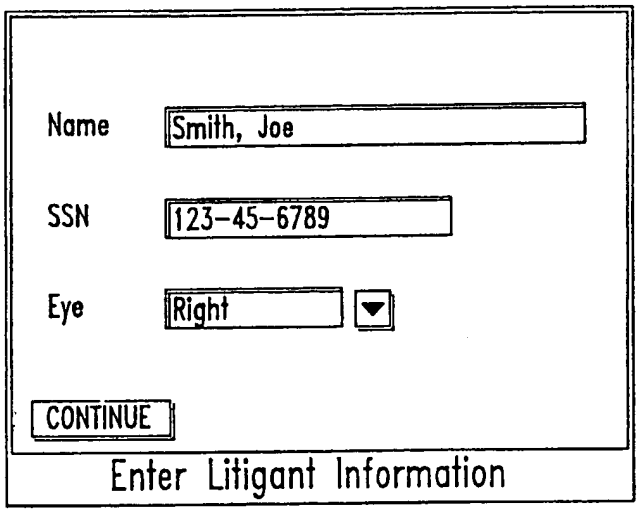

Name
Smith, Joe
SSN
123-45-6789
Eye
Right
CONTINUE
Enter Litigant Information

Fig. 15

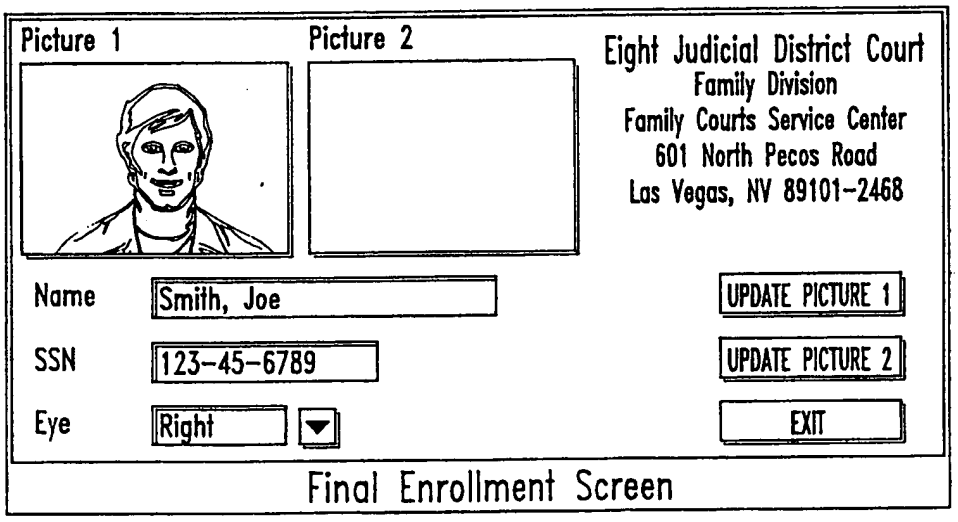

Picture 1
Picture 2
Eight Judicial District Court
Family Division
Family Courts Service Center
601 North Pecos Road
Las Vegas, NV 89101-2468
Name
Smith, Joe
SSN
123-45-6789
Eye
Right
UPDATE PICTURE 1
UPDATE PICTURE 2
EXIT
Final Enrollment Screen

Fig. 16

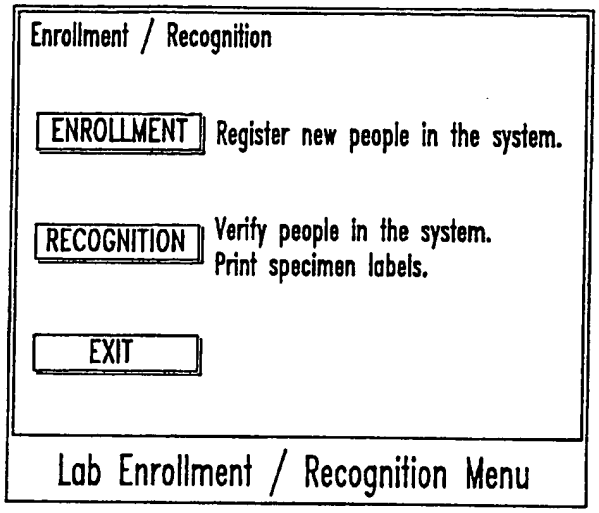

Enrollment / Recognition
ENROLLMENT
Register new people in the system.
RECOGNITION
Verify people in the system.
Print specimen labels.
EXIT
Lab Enrollment / Recognition Menu

Fig. 17

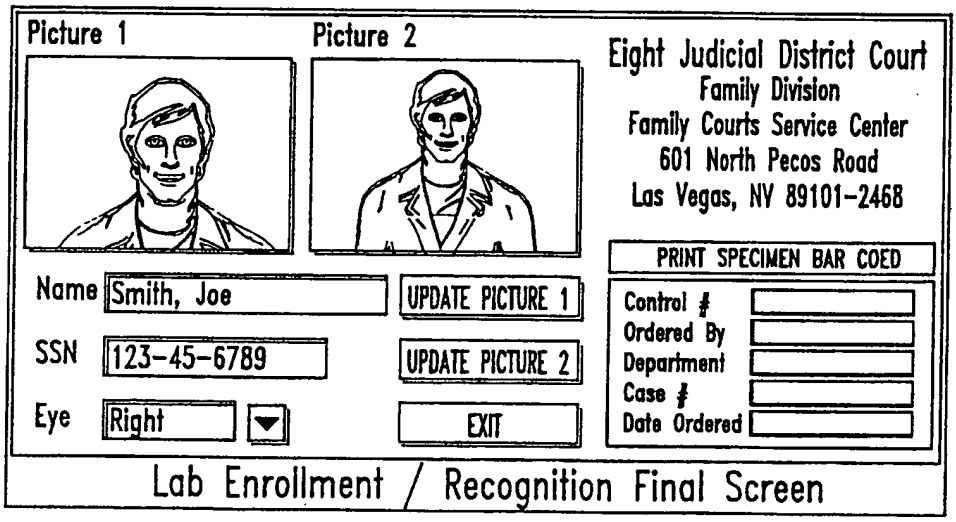

Picture 1
Picture 2
Eight Judicial District Court
Family Division
Family Courts Service Center
601 North Pecos Road
Las Vegas, NV 89101-2468
PRINT SPECIMEN BAR CODED
Name
Smith, Joe
UPDATE PICTURE 1
SSN
123-45-6789
UPDATE PICTURE 2
Eye
Right
EXIT
Control #
Ordered By
Department
Case #
Date Ordered
Lab Enrollment / Recognition Final Screen

Fig. 18

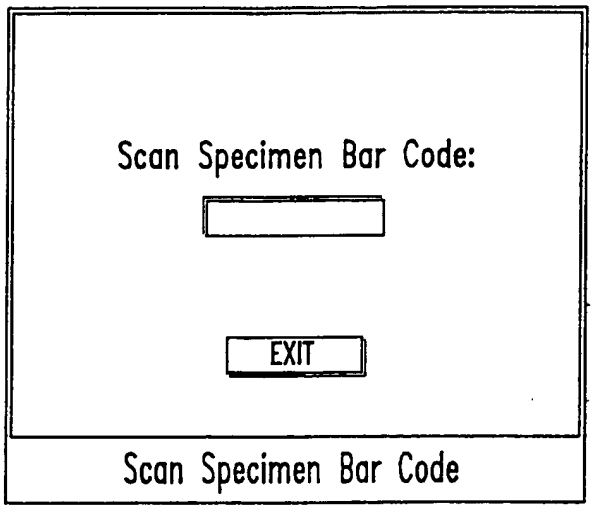

Scan Specimen Bar Code:
EXIT
Scan Specimen Bar Code

Fig. 19

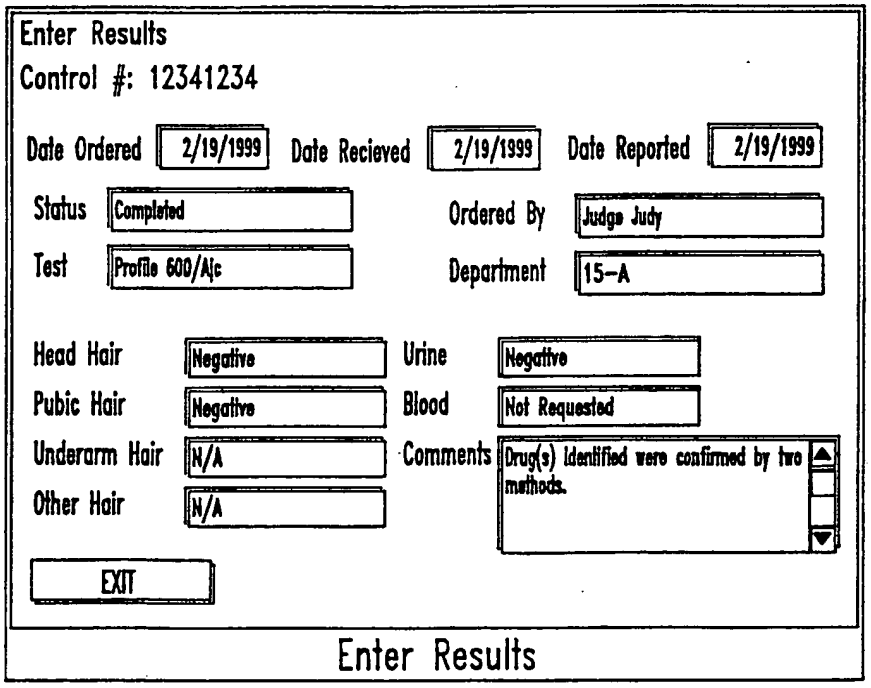

Enter Results
Control #: 12341234
Date Ordered 2/19/1999
Date Recieved 2/19/1999
Date Reported 2/19/1999
Status Completed
Ordered By Judge Judy
Test Profile 600/A|c
Department 15-A
Head Hair Negative
Urine Negative
Pubic Hair Negative
Blood Not Requested
Underarm Hair N/A
Comments Drug(s) identified were confirmed by two methods.
Other Hair N/A
EXIT
Enter Results

Fig. 20

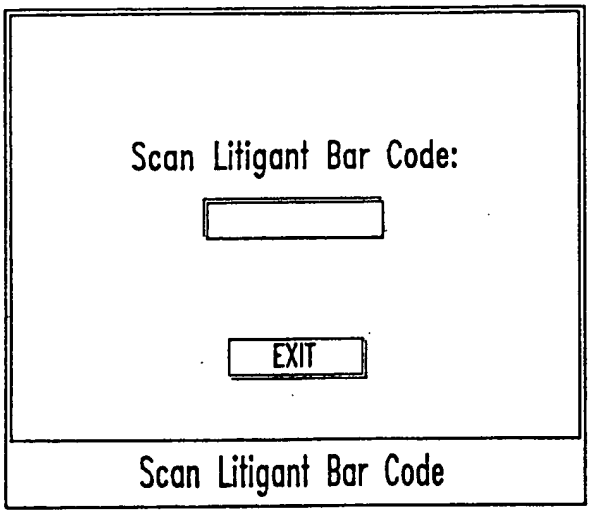

Scan Litigant Bar Code:
EXIT
Scan Litigant Bar Code

Fig. 21

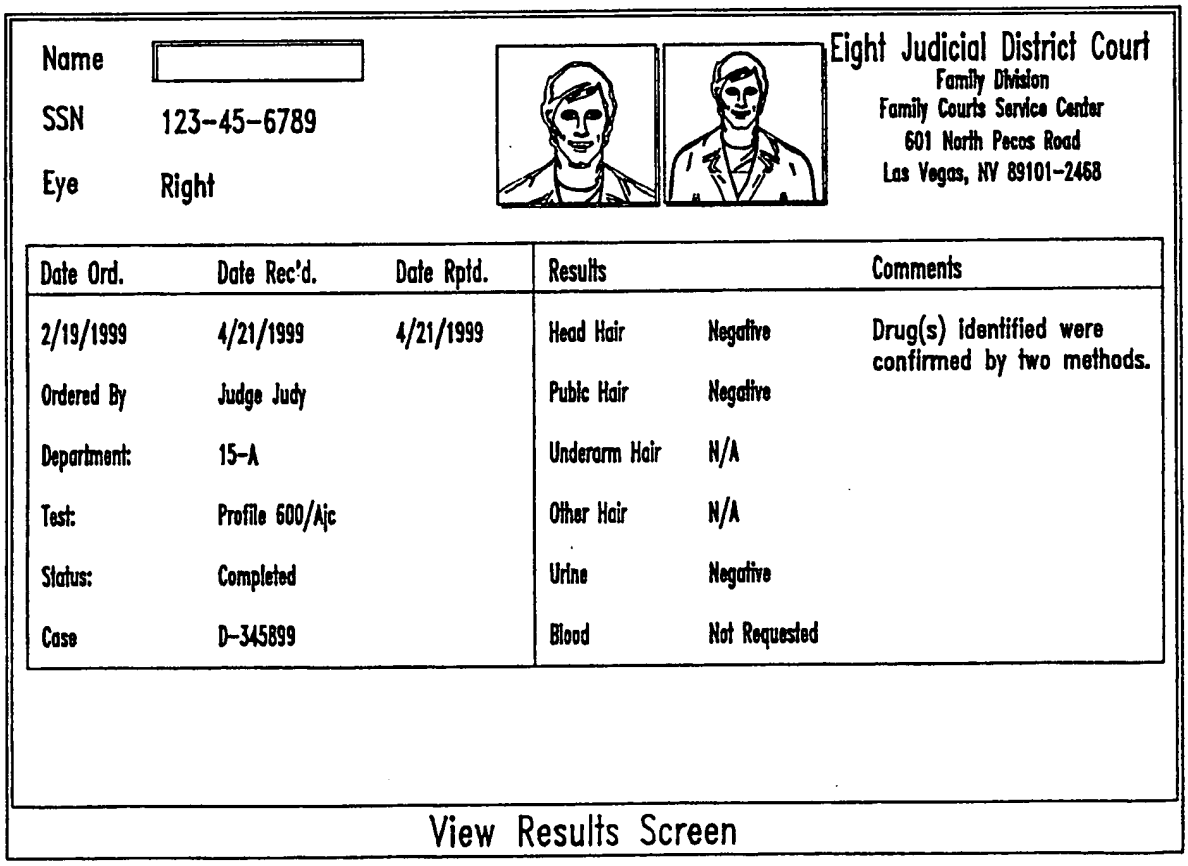

Name
SSN 123-45-6789
Eye Right
Eight Judicial District Court
Family Division
Family Courts Service Center
601 North Pecos Road
Las Vegas, NV 89101-2468
Date Ord. Date Rec'd. Date Rptd.
2/19/1999 4/21/1999 4/21/1999
Ordered By Judge Judy
Department: 15-A
Test: Profile 600/Ajc
Status: Completed
Case D-345899
Results
Head Hair Negative
Public Hair Negative
Underarm Hair N/A
Other Hair N/A
Urine Negative
Blood Not Requested
Comments
Drug(s) identified were confirmed by two methods.
View Results Screen

Fig. 22

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/13049

**A. CLASSIFICATION OF SUBJECT MATTER**

IPC(6) :G06K 9/00
US CL :382/116, 306; 707/9
According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 250/556, 557; 283/68, 69, 70, 77, 78, 81-114; 340/825.34; 356/71; 358/403; 382/115-127, 232, 306; 707/6, 9;

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST, IEEE

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X<br>---<br>Y | US 5,191,611 A (LANG) 02 March 1993, col. 1, line 45 - col. 2, line 67, col. 7, lines 14-17, col. 8, lines 1-3, col. 14, lines 5-10, col. 15, lines 25-27. | 1, 5, 6, 10, 11, 31-34<br>---<br>2-4, 7-9, 12-14, 16-19, 24-30 |
| Y | US 5,490,217 A (WANG et al) 06 February 1996, col. 2, lines 26-67, col. 3, line 15-22, col. 4, lines 13-17, col. 5, lines 5-10 and 40-55. | 4, 9, 12-14, 16-19, 24-30. |
| Y | US 5,513,272 A (BOGOSIAN, Jr.) 30 April 1996, figure 1. | 2, 3, 7, 8, 12-14, 16-19, 24-30 |

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

| | | | |
|---|---|---|---|
| * | Special categories of cited documents: | "T" | later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention |
| "A" | document defining the general state of the art which is not considered to be of particular relevance | "X" | document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone |
| "E" | earlier document published on or after the international filing date | "Y" | document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| "L" | document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | "&" | document member of the same patent family |
| "O" | document referring to an oral disclosure, use, exhibition or other means | | |
| "P" | document published prior to the international filing date but later than the priority date claimed | | |

| | |
|---|---|
| Date of the actual completion of the international search<br>25 OCTOBER 1999 | Date of mailing of the international search report<br>18 NOV 1999 |
| Name and mailing address of the ISA/US<br>Commissioner of Patents and Trademarks<br>Box PCT<br>Washington, D.C. 20231<br>Facsimile No. (703) 305-3230 | Authorized officer<br>BRIAN P. WERNER<br>Telephone No. (703) 305-3800 |

Form PCT/ISA/210 (second sheet)(July 1992)★

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/13049

**Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)**

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-19 and 24-34

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/13049

**Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)**

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-19 and 24-34

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.